

Original citation:

Beynon, W. M. (1981) On Raney's binary encoding for continued fractions, generalisations of Pell's Equation, and the theory of factorisation. Coventry, UK: Department of Computer Science. (Theory of Computation Report). CS-RR-034

Permanent WRAP url:

<http://wrap.warwick.ac.uk/47220>

Copyright and reuse:

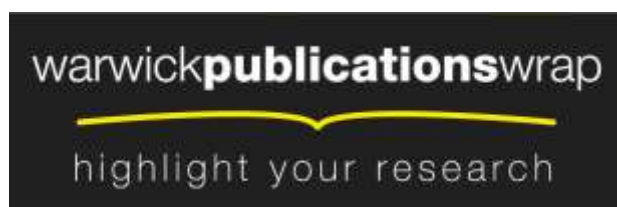
The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions. Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

A note on versions:

The version presented in WRAP is the published version or, version of record, and may be cited as it appears here.

For more information, please contact the WRAP Team at: publications@warwick.ac.uk



<http://wrap.warwick.ac.uk/>

The University of Warwick

THEORY OF COMPUTATION

REPORT NO.34

ON RANEY'S BINARY ENCODING FOR CONTINUED
FRACTIONS, GENERALISATIONS OF PELL'S
EQUATION, AND THE THEORY OF FACTORISATION

BY

W.M. BEYNON

Department of Computer Science
University of Warwick
COVENTRY CV4 7AL
ENGLAND.

January 1981

On Raney's binary encoding for continued fractions,
generalisations of Pell's equation,
and the theory of factorisation

by

W.M.Beynon

Introduction

Raney's algorithm for computing the continued fraction expansion of $(ax+b)/cx+d$ from the continued fraction expansion of x was first described in [R]. In that paper, a simple binary encoding for continued fraction expansions is of fundamental importance. In some sense, the study of this encoding - which is fully described in §1 below - is the unifying idea underlying this paper. The first five sections of the paper cover essentially the same ground as [R], but adopt a perspective in which the algorithm is the central object of interest. As far as the mathematical results are concerned, any originality is confined to presentation and organisation, and the most novel aspects of these sections are concerned with the formulation and justification of the algorithm and its derivatives. Of particular interest is the use of Dijkstra's guarded command notation [Di], a formalism ideally suited for expressing Raney's algorithm in its non-deterministic form (Algorithm 3.4).

The remaining sections of the paper are only tangentially related to Raney's algorithm, and apparently have greater originality. The main results are concerned with the encodings of continued fraction expansions of quadratic irrationals. The analysis of a modified form of Raney's algorithm (Algorithm 6.4) shows that encodings of positive quadratic irrationals with a negative algebraic conjugate are purely periodic, and that the period of this encoding is palindromic if and only if the associated quadratic irrational is the square root of a rational. Some elementary classical results on the periodicity of continued fraction expansions (see Cor's 6.4.5 and 6.4.8) and on the solution of Pell's equation (Prop.7.1) appear here in a slightly unusual perspective, and provide evidence that Raney's encoding is a natural representation of continued fractions. In confirmation of this, the study of necessary and sufficient conditions for the palindromic periods of square roots of rational numbers to be of odd or even length leads to apparently new results which relate the form of the continued fraction expansion of $\sqrt{b/c}$ to the solubility of a 'generalised Pell's equation' of the form:

$$Bx^2 - Cy^2 = c \text{ (even length) or } 2c \text{ (odd length)}$$

subject to $BC=bc$, and other constraints. (See Prop.'s 8.1 and 9.1). When $c=1$ and the encoding of \sqrt{b} has palindromic period of even length, the case $B=b$ and $C=1$ is of special interest, since it corresponds to the case when the numerical period of \sqrt{b} has odd length. (See §7).

Some elementary number-theoretic consequences of these results are explored in §10. The encodings of square roots of primes are characterised (Cor.10.1.2), and a classification of encodings of square roots of products of the form pq , where p and q are prime, is also given. A relationship between the computation of the continued fraction expansion of square roots of integers and the problem of factorisation is also discussed, and a novel heuristic factorisation technique is presented (Algorithm 10.2). The significant question in this context is whether, for large n , a multiplier k can be chosen in such a way that the computation of the periodic part of \sqrt{kn} is a feasible computation leading to a non-trivial factorisation of kn . In the special case $n=pq$, where p and q are primes of the form $4t+3$, the feasibility of the computation of the periodic part of \sqrt{n} would be sufficient to guarantee that the factorisation of n is feasible.

Acknowledgements.

I wish to thank David Fowler and Mike Paterson for many helpful conversations on the subject of this paper. I am indebted to Mike Paterson for the formulation of Raney's algorithm for double-balanced matrices which appears as Algorithm 4.2, and for observations which led to Corollaries 9.1.4 and 5.

I am also grateful to Mike Flynn and Pete Cameron for technical advice and help in preparing the paper.

Finally, I wish to thank the Nuffield Foundation for funds which enabled me to attend a series of lectures by Edsger Dijkstra at Santa Cruz in August 1979. But for this support, this paper would most certainly have been written differently - if indeed it had been written at all.

Index

- \$ 1. An encoding mechanism for positive reals.
- \$ 2. Homographic transformations and related properties of 2×2 matrices.
- \$ 3. Raney's algorithm and its justification.
- \$ 4. The structure of R_n, C_n and D_n and its operational significance.
- \$ 5. Raney's transducers.
- \$ 6. Fixpoints of $R(M,)$ and the expansions of quadratic irrationals.
- \$ 7. Pell's equation and the parity of palindromic encodings.
- \$ 8. Even palindromic encodings.
- \$ 9. Odd palindromic encodings.
- \$10. Some number-theoretic consequences.

\$1. An encoding mechanism for positive reals

The first five sections of this paper, which are closely based on [R], are concerned with the formulation and justification of Raney's algorithm for the solution of the following problem:

Given a real number x as a continued fraction, and integers a, b, c, d , find the continued fraction expansion of $(ax + b)/(cx + d) = y$.

Notation:

The set of non-negative real numbers, together with ∞ will be denoted by R^∞ . If M is the 2×2 integer matrix:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

then $M[x]$ will denote $(ax+b)/(cx+d)$. The map $M[]$ is then a homographic transformation, and x and $M[x]$ are homographically related.

The class of 2×2 matrices M with non-negative integer entries and a positive determinant (respectively positive determinant n) will be denoted by P (respectively P_n). The matrices:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

in P_1 will be denoted by U and L respectively.

For reasons to be discussed later (see the Remark after Prop.2.1), it suffices to consider the problem of computing the continued fraction expansion of $y=M[x]$, where x is in R^∞ , and M is in P . In this case, y is also in R^∞ . Raney's solution to this problem makes essential use of an encoding which associates with each element of R^∞ at least one infinite string in the alphabet $A = \{u, l\}$.

To define Raney's encoding, consider first the map $e: A^* \rightarrow Q^+$ mapping $u^a l^b u^c \dots (u \text{ or } l)^z$ to $[a; b, c, \dots, z]$,

where $a \geq 0$, and $b, c, \dots, z > 0$. If p is an infinite string in the alphabet A , and p_n is the prefix consisting of the first n symbols of p , then elementary analysis will show that $e(p_n)$ tends to a limit $E(p)$ as n tends to infinity (c.f. [D] p.88). If A^∞ denotes the set of infinite strings in the alphabet A , a map $E: A^\infty \rightarrow R^\infty$ is defined in this way. If x is in R^∞ , and $E(p)=x$, then p is an encoding of x .

Proposition 1.1:

- (i) The image of E is R^∞
- (ii) $0, \infty$ and all positive irrationals have a unique encoding
- (iii) A positive rational has precisely two encodings, one having suffix lu^∞ , the other ul^∞ .

Proof:

(i) and (ii) If x is a positive irrational, it has a unique non-terminating continued fraction expansion $[a_0; a_1, a_2, \dots, a_n, \dots]$. (See [D] p.88-92). Thus by elementary analysis:

$$x = \lim_{n \rightarrow \infty} [a_0; a_1, \dots, a_n] = E(u^{a_0} l^{a_1} u^{a_2} \dots).$$

If $x = m/n$ where m and $n \in \mathbb{Z}^+$, then x has a terminating continued fraction expansion $[a_0; a_1, \dots, a_k]$, where a_0, a_1, \dots, a_k are the successive quotients in the division form of Euclid's algorithm applied to the pair (m, n) , and $a_k \geq 2$. (See e.g. [K] p.316-320). Thus

$$x = \lim_{m \rightarrow \infty} [a_0; a_1, \dots, a_k, m] = \lim_{m \rightarrow \infty} [a_0; a_1, \dots, a_k - 1, 1, m]$$

and x has two encodings given by concatenating $u^{a_0} l^{a_1} \dots (u \text{ or } l)^{a_k-1}$ with ul^∞ and lu^∞ .

The above analysis deals with all infinite strings in the alphabet A other than u^∞ and l^∞ , which are the encodings of ∞ and 0 respectively.

Remark:

If $x = m/n$ where m and n are positive integers, then Euclid's algorithm for computing $g = \text{GCD}(m, n)$, in its subtraction form, generates a sequence of matrices S_1, S_2, \dots, S_t , where $S_i \in \{L, U\}$, such that

$$\begin{pmatrix} m \\ n \end{pmatrix} = S_1 \dots S_t \begin{pmatrix} g \\ g \end{pmatrix}.$$

If $s_i =$ (if $S_i = L$ then l else u), then a simple extension of the above proof shows that $s_1 \dots s_t u l^\infty$ and $s_1 \dots s_t l u^\infty$ are the two encodings of x .

Cor.1.1.1:

If p is in A^∞ , then:

- (i) If \bar{p} is obtained from p by interchanging l and u , then $E(\bar{p}) = (E(p))^{-1}$
- (ii) $E(u.p) = 1 + E(p) \geq 1$
- (iii) $E(l.p) = E(p)/(1 + E(p)) \leq 1$

Proof:

(i) If $a_c = \emptyset$, then $[a_c; a_1, \dots, a_n]^{-1} = [\emptyset; a_c, a_1, \dots, a_n]$, so that $[\emptyset; a_1, \dots, a_n]^{-1} = [a_1; a_1, \dots, a_n]$. Thus, interchanging l and u in a string q in A^* gives \bar{q} such that $e(\bar{q}) = (e(q))^{-1}$. But then

$$E(\bar{p}) = \lim_{k \rightarrow \infty} e(\bar{p}_k) = \lim_{k \rightarrow \infty} (e(p_k))^{-1} = (E(p))^{-1}$$

(To eliminate trivial arguments with limits, this proof may be paraphrased

" $E(p) = [a; b, c, \dots] \Rightarrow$

$(E(p))^{-1} =$ if $a > \emptyset$ then $[\emptyset; a, b, c, \dots]$ else $[a; b, c, \dots] = E(p)$ "

This abbreviated form of argument is used for (ii) and (iii)).

- (ii) $E(u.p) = [a; b, c, \dots]$ where $a > \emptyset$
 $= 1 + [a-1; b, c, \dots]$
 $= 1 + E(p)$

- (iii) Suppose $E(l.p) = [\emptyset; a, b, c, \dots]$ where $a > 1$
 $= [a; b, c, \dots]^{-1}$

Then $E(p) = \begin{cases} [\emptyset; a-1, b, c, \dots] & \text{if } a > 1 \\ [b; c, \dots] & \text{if } a = 1 \end{cases}$

Hence $(E(p))^{-1} = \begin{cases} [a-1; b, c, \dots] & \text{if } a > 1 \\ [\emptyset; b, c, \dots] & \text{if } a = 1 \end{cases}$

and $E(l.p) = (1 + (E(p))^{-1})^{-1} = E(p)/(1 + E(p))$.

§2. Homographic transformations and related properties of 2x2 matrices

Raney's algorithm is based upon relationships between the homographic transformations defined by a 2x2 integer matrix M and the matrices UM , LM , MU and ML (see Prop.2.1 and Algorithm 3.1). The other results of this section will be used to give qualitative information about the behaviour of Algorithm 3.1.

Prop. 2.1:

Let M be a 2x2 integer matrix, and $x \in \mathbb{R}^\infty$. Then

- (i) $UM[x] = 1 + M[x]$
- (ii) $LM[x] = 1/(1 + 1/M[x])$
- (iii) $MU[x] = M[1 + x]$
- (iv) $ML[x] = M[x/(1+x)]$

Proof:

- (i) $UM[x] = ((a + c)x + (b + d))/(cx + d)$
 $= 1 + (ax + b)/(cx + d)$
 $= 1 + M[x]$
- (ii) $LM[x] = (ax + b)/((a + c)x + b + d) = 1/(1 + 1/M[x])$
- (iii) $MU[x] = (ax + (a+b))/(cx + (c + d)) = (a(x+1) + b)/(c(x+1) + d)$
- (iv) $ML[x] = ((a+b)x + b)/((c+d)x + d)$
 $= (ax + b(x+1))/(cx + d(x+1))$
 $= (a(x/(1+x)) + b)/(c(x/(1+x)) + d)$
 $= M[x/(1+x)]$

Remark: Prop.2.1 can be used to show that the general problem of computing the continued fraction expansion of $M[x]$ as originally presented can be reduced to the case $M \in P$ and $x \in \mathbb{R}^\infty$. Such a reduction is proposed in [R], but this fails in special cases (e.g. $a = d = 0$ and $b < 0$, when Step (e) fails to achieve $b \geq 0$). (See Appendix 1).

Prop.2.2: Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in P$

- (i) $U^{-1}M \in P \iff a \geq c$ and $b \geq d$
- (ii) $L^{-1}M \in P \iff a \leq c$ and $b \leq d$
- (iii) $MU^{-1} \in P \iff a \geq b$ and $c \geq d$
- (iv) $ML^{-1} \in P \iff a \leq b$ and $c \leq d$

Proof:

(i) If $a \geq c$ and $b \geq d$, then $U^{-1}M = \begin{pmatrix} a-c & b-d \\ c & d \end{pmatrix} \in P$.

Conversely, if $U^{-1}M = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in P$ then $M = \begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix}$ where p and q are ≥ 0 .

The proofs of (ii), (iii) and (iv) are equally simple.

Definition: Let $M \in P$. Then

M is row-balanced if neither $U^{-1}M$ nor $L^{-1}M$ is in P .

M is column-balanced if neither MU^{-1} nor ML^{-1} is in P .

M is double-balanced if it is both row- and column-balanced.

Notation:

The subclasses of P consisting of row-, column-, and double-balanced matrices will be denoted by RB , CB , and DB respectively. For $n > 0$, the notation RB_n (respectively CB_n , DB_n) will be used to denote the subclass of RB (respectively CB , DB) consisting of matrices of determinant n .

Lemma 2.3: Let $X, Y \in P$.

- (i) $XY \in RB \implies X \in RB$
- (ii) $XY \in CB \implies Y \in CB$

Proof:

(ii) If neither XYU^{-1} nor XYL^{-1} is in P then neither YU^{-1} nor YL^{-1} is in P .
 (i) is similar.

Cor. 2.2.1: In the notation of Prop. 2.2:

- (i) M is row-balanced iff $a > c$ and $d > b$
- (ii) M is column-balanced iff $a > b$ and $d > c$

Proof: Evident since $ad - bc > 0$.

Cor. 2.2.2:

- (i) If $X \notin P$ then UX or $LX \notin P$.
- (ii) If $X \notin P$ then XU or $XL \notin P$.
- (iii) If $X \in P$ then $U^{-1}X$ or $L^{-1}X \notin P$.
- (iv) If $X \in P$ then XU^{-1} or $XL^{-1} \notin P$.

Proof: (i) Each element of X appears in UX or LX , and if X has a negative entry then so also does UX or LX . Moreover, $\det UX = \det LX = \det X$. The proof of (ii) is similar.

(iii) $U^{-1}X$ and $L^{-1}X \in P \Rightarrow \det X = 0$ by Prop. 2.2. The proof of (iv) is similar.

Cor. 2.2.3: If $X \in P$ then

- (i) $L^{-1}X \notin P$ and $L^{-1}XL \in P \Rightarrow L^{-1}XL \in CB$
- (ii) $U^{-1}X \notin P$ and $U^{-1}XU \in P \Rightarrow U^{-1}XU \in CB$

Proof: (i) $(L^{-1}XL)L^{-1} = L^{-1}X \notin P$. But also $XLU^{-1} \notin P$ (Cor. 2.2.2 (ii)) whence $(L^{-1}XL)U^{-1} \notin P$.

(ii) is similar

Cor. 2.2.4: If $M \in P$ then

- (i) M has a canonical expression of the form:
 $S_1 S_2 \dots S_t M_R$ where $M_R \in RB$, each $S_i = L$ or U , and $t \geq 0$.
- (ii) M has a canonical expression of the form:
 $M_C T_1 T_2 \dots T_s$ where $M_C \in CB$, each $T_i = L$ or U , and $s \geq 0$.

Proof: (i) If $M \in RB$ then $t=0$. Otherwise, either $U^{-1}M$ or $L^{-1}M \in P$, but not both, whence $M = S(S^{-1}M)$ where $S = L$ or U , and $S^{-1}M \in P$. But sum of coefficients of $S^{-1}M < \text{sum of coefficients of } M$ and a canonical factorisation of M as $S_1 S_2 \dots S_t M_R$ results from repeated extraction of left factors of M .

(ii) is similar.

Cor. 2.2.5: (i) If $M \in RB$ then $M_C \in DB$

(ii) If $M \in CB$ then $M_R \in DB$

Proof: (i) $M = M_C T$ and $M \in RB \Rightarrow M_C \in RB$ by Lemma 2.3

Notation: 'cap' will be used to denote the unique map from the free monoid A^* to P_1 induced by defining $\text{cap}(u) = U$ and $\text{cap}(l) = L$.

Cor. 2.2.6: 'cap' is an isomorphism of monoids.

Proof: $M \in P_1 \Rightarrow M = S_1 S_2 \dots S_t$ uniquely, since:
 $DB_1 = RB_1 = CB_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$
 $\Rightarrow M = \text{cap}(s_1 s_2 \dots s_t)$ uniquely,
 where $s_i = \begin{cases} l & \text{if } S_i = L \\ u & \text{if } S_i = U \end{cases}$

\$3. Raney's algorithm and its justification

Raney's algorithm accepts as input an infinite string p in A^∞ , where $E(p) = x$, and a matrix M in P , and outputs q in A^∞ , where $E(q) = y$, and $M[x] = y$. Thus, if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then Raney's algorithm effectively computes

the continued fraction expansion of $(ax+b)/(cx+d)$ from the continued fraction expansion of x . The algorithm can conveniently be described in the "guarded command" notation developed by E.W.Dijkstra. (see e.g. [Di]). Loop invariants are enclosed within parentheses ($\{ \dots \}$), and 'in' and 'out' are used to denote the prefix of the input currently accepted and the prefix of the output currently given, respectively.

Algorithm 3.1: "Raney's algorithm"

```

< p := ualbuc... where x = [a;b,c, ...] >;
M := M0; {M0 ∈ P}
do true →
  dow M ∉ RB →
    { M0.cap(in) = cap(out).M }
    if U-1M ∈ P → <output 'u'>; M := U-1M
    [] L-1M ∈ P → <output 'l'>; M := L-1M
    fi
  od;
  dor M ∈ RB →
    { M0.cap(in) = cap(out).M }
    < read s, the next symbol of p >;
    if s = 'u' → M := MU
    [] s = 'l' → M := ML
    fi
  od
od

```

Before proving the correctness of Raney's algorithm, it is necessary to establish basic facts about its behaviour. A priori, the algorithm might accept input indefinitely without giving an output, for instance. Since there are two possible encodings of a rational number, there is also an a priori possibility of non-determinism in the output. (A possibility admitted in Dijkstra's notation, in which a non-deterministic choice between alternatives in a do or if clause is made when more than one guard is true).

Since $\det U = \det L = 1$, the determinant of M is invariant under all assignments to M in the algorithm. As this fact suggests, there is a relationship between the behaviour of Raney's algorithm and the algebraic properties of matrices in P with fixed determinant $n > 0$.

Cor. 2.2.7 (to Prop. 2.2): For $n > 0$:

- (i) if $M \in RB_n, CB_n$ or DB_n then the trace of M , $\text{tr}(M) \leq n+1$
and (ii) the classes RB_n, CB_n and DB_n are finite.

Proof:

- (i) $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in RB \iff p > r \geq 0 \text{ and } s > q \geq 0 \text{ and } ps - qr = n$
 $\iff p > r \geq 0 \text{ and } s > q \geq 0 \text{ and } n \geq ps - (p-1)(s-1)$
 $\iff p > r \geq 0 \text{ and } s > q \geq 0 \text{ and } n \geq p+s-1$
(ii) Only finitely many values of p and s satisfy $n \geq p+s-1$.

Prop. 3.2: In the execution of Raney's algorithm with input parameters $p \in A^\infty$ and $M \in P$:

- (i) There is no non-determinism in loop W.
- (ii) Loop R can be iterated only finitely many times without output being given.
- (iii) Loop W can be iterated only finitely many times without input being read.
- (iv) When loop W terminates, the next symbol to be output is ambiguous. In particular, the next output will be 'u' (resp. 'l') if the subsequent input is 'u' (resp. 'l').

Proof: Suppose that $\det M = n > 0$.

(i) Loop W gives output non-deterministically only if at some stage both $U^t M$ and $L^t M$ are in P , which is impossible by Cor. 2.2.2.

(ii) Since the assignments $M := MU$ and $M := ML$ both strictly increase the determinant of M (again using $\det M \neq 0$), a sequence of k successive iterations of loop R without output generates k distinct matrices in RB_n . Thus k is finite by Cor. 2.2.7.

(iii) See Cor. 2.2.3 (ii)

(iv) On termination of loop W, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a > c$ and $d > b$.

(See Cor. 2.2.1). In the sequence of matrices M, MU, MU^2, \dots , the first matrix not in RB_n is of the form:

$$MU^n = \begin{pmatrix} a & b+ra \\ c & d+rc \end{pmatrix}$$

where $a \geq c$ and $b+ra \geq d+rc$. Thus if the next segment of input is a sufficiently large block of 'u' 's, the next output symbol will be 'u'. Similarly, if the subsequent input is a sufficiently large block of 'l' 's, the next output symbol will be 'l'.

Cor. 3.2.1: For given input parameters p in A^∞ and M_0 in P , Raney's algorithm outputs a uniquely determined string $R(M_0, p)$ in A^∞ . Hence the algorithm computes a well-defined function $R: P \times A^\infty \rightarrow A^\infty$.

The justification of Algorithm 3.1.

The formulation of Raney's algorithm given previously has conceptual advantages which will become apparent. From the point of view of proving correctness, it is helpful to observe that precisely the same effect is obtained by a simpler version of Algorithm 3.1, viz:

```

do  $M \notin RB \rightarrow$ 
  if  $U^t M \in P \rightarrow$  <output 'u'>;  $M := U^t M$ 
  if  $L^t M \in P \rightarrow$  <output 'l'>;  $M := L^t M$ 
fi
if  $M \in RB \rightarrow$ 
  <read s, next symbol of p>;
  if  $s = 'u' \rightarrow M := MU$ 
  if  $s = 'l' \rightarrow M := ML$ 
fi
od
```

From this formulation it is apparent that $R(M, p)$ is the element of A^∞ with the recursive definition:

```

 $R(M, p) =$  if  $M \notin RB \rightarrow$ 
  if  $U^t M \in P \rightarrow u. R(U^t M, p)$ 
  if  $L^t M \in P \rightarrow l. R(L^t M, p)$ 
fi
if  $M \in RB \rightarrow$ 
  if  $p = u.q \rightarrow R(MU, q)$ 
  if  $p = l.q \rightarrow R(ML, q)$ 
fi
fi
```

To prove the correctness of Raney's algorithm is equivalent to proving that $E(R(M,p)) = M[E(p)]$. From the recursive definition of R above, and Cor. 1.1.1 it follows that $E(R(M,p)) = r(M,p)$ in R^∞ , where

$$\begin{aligned}
 r(M,p) = & \text{if } M \notin RB \rightarrow \\
 & \quad \text{if } U^1 M \in P \rightarrow 1 + r(U^1 M, p) \\
 & \quad \quad \text{if } L^1 M \in P \rightarrow 1/(1 + 1/r(L^1 M, p)) \\
 & \quad \text{fi} \\
 & \text{if } M \in RB \rightarrow \\
 & \quad \text{if } p = u.q \rightarrow r(MU, q) \\
 & \quad \quad \text{if } p = l.q \rightarrow r(ML, q) \\
 & \quad \text{fi} \\
 & \text{fi}
 \end{aligned}$$

Patently, this recursive equation specifies a unique number $r(M,p)$ in R^∞ for any choice of M and p , namely, the limiting value of $e(p_n)$ as n tends to infinity, where p_n is the prefix of $R(M,p)$ of length n . But Prop. 2.1 shows that $M[E(p)]$ satisfies the equation. This proves:

Theorem 3.3: Raney's algorithm is correct:

if $M \in P$ and $p \in A^\infty$, then $E(R(M,p)) = M[E(p)]$

Remark: The use of an "if ... \square ... fi" construct in the recursive definitions above should not be confused with the alternative construct introduced by Dijkstra. (See [Di] p.33-34), even though the same non-deterministic selection between true guards in interpreting the definitions is intended. A more conventional recursive definition of $R(M,p)$ is:

$$\begin{aligned}
 R(M,p) = & \text{if } M \notin RB \text{ then} \\
 & \quad \text{if } U^1 M \in P \text{ then } u. R(U^1 M, p) \text{ else } l. R(L^1 M, p) \text{ fi} \\
 & \text{else} \\
 & \quad \text{if } p = s.q \text{ and } s = u \text{ then } R(MU, q) \text{ else } R(ML, q) \text{ fi} \\
 & \text{fi}
 \end{aligned}$$

which is both obscure and inelegant.

Cor. 3.2.2: If $M \in P$, the mapping $R(M,): A^\infty \rightarrow A^\infty$ is 1-1. The string p in A has suffix l^∞ (resp. u^∞) iff $R(M,p)$ also does.

Proof: Suppose that p and q in A^∞ are such that $R(M,p) = R(M,q)$. Then, by Theorem 3.3, $M[E(p)] = M[E(q)]$, whence $E(p) = E(q)$, as M is non-singular.

If $E(p)$ is irrational or \emptyset or ∞ , then $p=q$ by Prop. 1.1 (ii). Suppose then that $E(p)$ is rational, and that p ends (wlog) in u^∞ . Clearly, $E(R(M,p))$ is then also rational, and by Prop. 3.2 (iv), the string $R(M,p)$ ends in u^∞ . That is, $R(M,q)$ ends in u^∞ . By Prop. 3.2 (iv) again, q ends in u^∞ , which suffices to prove that $p=q$ by Prop. 1.1 (iii).

Remark: It is easy to show that $R(M,)$ is bijective iff M is diagonal with positive entries. Only if M has this simple form is the map $M[]$ a surjection.

It is interesting to compare Algorithm 3.1 with the following non-deterministic algorithm:

Algorithm 3.4: "A non-deterministic version of Raney's algorithm"

```

< p := ualbuc... where x = [a;b,c, ... ] >;
M := M0; {M0 ∈ P}
do { M0.cap(in) = cap(out).M }
  U-1M ∈ P → <output 'u'>; M := U-1M
  || L-1M ∈ P → <output 'l'>; M := L-1M
  || true → < read s, the next symbol of p >;
    if s = 'u' → M := MU
    || s = 'l' → M := ML
    fi
  od

```

In this algorithm, it is possible that no output is given at any stage; indeed, there are execution sequences in which the output sequence is of any specified length.

Theorem 3.5: In any execution sequence of Algorithm 3.4, the output is a string q in $A^* \cup A^\infty$ such that q is a prefix of $R(M,p)$.

Proof: First consider Algorithm 3.1, which is in effect Algorithm 3.4 with a particular execution sequence imposed. If p_k denotes the k -th input symbol, then $M_0.\text{cap}(p_1 \dots p_k) = W.M_R$ where $M_R \in RB$ in canonical form (see Cor.'s 2.2.5 and 2.2.6), and $\text{cap}^{-1}(W)$ is a prefix of $R(M,p)$ because the invariant relationship $M_0.\text{cap}(\text{in}) = \text{cap}(\text{out}).M$ holds in loop R and loop W .

Now in a general execution sequence of Algorithm 3.4, the relation:

$$M_0.\text{cap}(\text{in}) = \text{cap}(\text{out}).M$$

is still invariant. Thus, if the input sequence 'in' so far accepted is $p_1 p_2 \dots p_k$, then the output sequence 'out' is a prefix of $\text{cap}(W)$ as defined above. Hence 'out' is at all times a prefix of $R(M,p)$.

Cor.3.5.1: If an execution sequence for Algorithm 3.4 generates an output string in A^∞ , then that string is $R(M,p)$.

Algorithm 3.1 is distinguished in the class of possible algorithms derived from the non-deterministic form above in that output is given as soon as it is available. In effect, this minimises the requirement for "remembering" the input string, and is central to the "finite state" nature of Algorithm 3.1 explored in §5.

\$4. The structure of RB_n, CB_n and DB_n and its operational significance.

Prop. 4.1: Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in P$. Then

- (i) $L^{-1}ML \in P \iff c+d \geq a+b$
- (ii) $U^{-1}MU \in P \iff c+d \leq a+b$
- (iii) $LML^{-1} \in P \iff a+c \geq b+d$
- (iv) $UMU^{-1} \in P \iff a+c \leq b+d$

Proof: (i) $L^{-1}ML = \begin{pmatrix} a+b & b \\ c+d-a-b & d-b \end{pmatrix}$

Thus $L^{-1}ML \in P$ iff $c+d \geq a+b$ and $d \geq b$.

But $ad-bc > 0$ and $c+d \geq a+b \Rightarrow d \geq b$.

(ii), (iii) and (iv) are similar.

Notation:

If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in RB$, then $p(M)$ (resp. $q(M)$) will denote $d-b$ (resp. $a-c$).

Cor. 4.1.1: Let $M \in RB$. Then

- (i) $ML \in RB \iff q(M) > p(M)$
- (ii) $MU \in RB \iff q(M) < p(M)$

Proof: (i) $q(M) > p(M) \iff a-c > d-b$
 $\iff a+b > c+d$
 $\iff L^{-1}ML \notin P$ by Prop.4.1.

Thus $ML \in RB \Rightarrow q(M) > p(M)$.

Conversely, $L^{-1}ML \notin P \Rightarrow U^{-1}MU \in P$ by Prop.4.1

$\Rightarrow U^{-1}ML \notin P$ by Cor.2.2.2(ii), since $U^{-1}M \notin P$
 $\Rightarrow ML \in RB$

(ii) is similar.

Cor. 4.1.2: Let $M \in RB$.

- (i) If $MU \in RB$ then $q(MU) = q(M)$, $p(MU) = p(M) - q(M) > 0$.

$$\text{Equivalently } \begin{pmatrix} p(M) \\ q(M) \end{pmatrix} = U \cdot \begin{pmatrix} p(MU) \\ q(MU) \end{pmatrix}$$

- (ii) If $ML \in RB$ then $p(ML) = p(M)$, $q(ML) = q(M) - p(M) > 0$.

$$\text{Equivalently } \begin{pmatrix} p(M) \\ q(M) \end{pmatrix} = L \cdot \begin{pmatrix} p(ML) \\ q(ML) \end{pmatrix}$$

Proof: (i) $MU \in RB \Rightarrow p(M) > q(M)$, by Cor.4.1.1.

If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $MU = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$, and hence:

$p(MU) = c+d-a-b = (d-b)-(a-c) = p(M) - q(M)$, and $q(MU) = a-c = q(M)$.

(ii) is similar.

Cor. 4.1.3:

Let $M \in RB$. There is a unique sequence of matrices S_1, \dots, S_t where each $S_i \in \{L, U\}$, such that t is maximal subject to the condition:

$$MS_1 \dots S_k \in RB \text{ for } 1 \leq k \leq t.$$

This sequence is such that

- (i) $\begin{pmatrix} p(M) \\ q(M) \end{pmatrix} = S_1 S_2 \dots S_t \begin{pmatrix} g \\ g \end{pmatrix}$ where $g = \text{GCD}(p(M), q(M))$

$$(ii) MS_1 \dots S_t = \begin{pmatrix} C+g & B \\ C & B+g \end{pmatrix}$$

- (iii) $E(\text{cap}^{-1}(S_1 S_2 \dots S_t) \cdot (lu^\infty \text{ or } ul^\infty)) = p(M)/q(M)$.

Proof: Cor.4.1.1 shows that if $M \in RB$, then at most one of ML and $MU \in RB$, which proves the uniqueness of a maximal sequence. Cor 4.1.2 shows that if $S(k)$ denotes S_1, S_2, \dots, S_k then:

$$\begin{pmatrix} p(M) \\ q(M) \end{pmatrix} = S(k) \begin{pmatrix} p(M.S(k)) \\ q(M.S(k)) \end{pmatrix} \text{ for } 1 \leq k \leq t$$

and that each successive post-multiplication by an S_i corresponds to a subtraction step in Euclid's subtraction algorithm for determining g . The form of MS_1, \dots, S_t given in (ii) is another consequence of Cor. 4.1.1, and (iii) follows from the remark after Prop. 1.1.

Cor.4.1.4: Let $n > 0$. There is a canonical 1-1 correspondence between matrices in DB_n and triples (B, C, g) of non-negative integers such that $(B+C+g).g = n$. In particular, DB_n has at least n elements, and has exactly n iff n is prime.

Proof: Let $M \in DB_n$. Associate with M the triple

$$(B, C, g) \text{ where } Q = \begin{pmatrix} C+g & B \\ C & B+g \end{pmatrix}$$

is the matrix derived from M as in Cor.4.1.3 (ii). The determinant of Q is $(C+g)(B+g) - BC = (B+C+g)g = n$. Conversely a triple (B, C, g) satisfying this condition naturally determines a matrix akin to Q having determinant n , and a unique double-balanced matrix D in DB_n can be derived by exploiting the canonical factorisation described in Cor.2.2.4.

Amongst the solutions of $(B+C+g)g = n$ are the n triples $(B, C, 1)$ such that $B+C+1 = n$. No other solutions are possible if n is prime. If n is composite there is a non-trivial factor $g \leq \sqrt{n}$, and triples (B, C, g) such that $B+C = n/g - g$ are solutions.

Cor.4.1.5: If $M \in RB$ then

- (i) $ML \in RB$ or $L^{-1}ML \in CB$
- and (ii) $MU \in RB$ or $U^{-1}MU \in CB$

Proof: (i) By Prop.4.1 and Cor.4.1.1, $ML \notin RB \Rightarrow L^{-1}ML \in P$. But, by Cor.2.2.3, this entails $L^{-1}ML \in CB$ since $L^{-1}M \notin P$.
(ii) is similar.

The results of Cor. 4.1.1 - 4.1.5 are sufficient to give an effective classification of CB_n, DB_n , and RB_n for each n . Cor. 4.1.4 shows that there is a unique matrix D in DB_n associated with each solution of $(B+C+g)g = n$. Cor. 2.2.5 shows that each row-balanced matrix is of the form $DS_1 \dots S_k$ for a unique D in DB_n , and Cor. 4.1.3 indicates how all row-balanced matrices of this form are derived from D . Since

$$M \in CB \Leftrightarrow M^T \in RB$$

and, in particular, $M \in DB$ entails $M^T \in DB$, there is a dual classification of column-balanced matrices. Thus if $C \in CB$, then $R = C^T \in RB$, whence:

$$\begin{aligned} R &= DS_1 \dots S_k \\ \text{and } C &= R^T = (DS_1 \dots S_k)^T \\ &= S_k^T \dots S_1^T D^T \end{aligned}$$

in canonical form. These arguments extend simply to prove a dual of Cor. 4.1.3, characterising column-balanced matrices of the form $T_1 \dots T_k D$, where each $T_i \in \{L, U\}$ and D is a given matrix in DB .

Notation:

Let $D \in DB$.

The sequence of row-balanced matrices

$$D, DS_1, DS_1 S_2, \dots, DS_1 S_2 \dots S_t$$

as defined above will be called a row-sequence.

The sequence of column-balanced matrices

$$T_1 \dots T_r D, T_1 \dots T_r D, \dots, D$$

as defined above will be called a column-sequence.

Remark: If $M \in RB$ (resp. CB) then M is in a unique row (resp. column) sequence, so that "the row (resp. column) sequence of M " is well-defined.

The above analysis is the basis for a more precise operational view of Algorithm 3.1. An iteration of the do true \rightarrow od clause will be called "a complete iteration" of the algorithm. By Prop. 3.2, each complete iteration comprises finitely many iterations of loop W - the "output phase" - followed by finitely many iterations of loop R - the "input phase". In some respects the first complete iteration may be exceptional. Initially M is in P ; after the first output phase (which can comprise an arbitrary number k iterations, as when $M = U^k N$ and $N \in RB$), the matrix M is in RB . At each iteration of the first input phase other than the last, M is replaced by the next matrix in the unique row-sequence to which it belongs. On the last iteration, M is replaced by MU (resp. ML) where MU (resp. ML) is in RB . Since this analysis depends only upon the premise that $M_0 \in P$, it is possible to deduce that prior to the execution of any complete iteration of Algorithm 3.1 other than the first, the assertion:

{ $M \in P \setminus RB$ and either the last input was u and $MU^{-1} \in RB$
or the last input was l and $ML^{-1} \in RB$ }

is valid. By Cor 4.1.5, it follows that in any complete iteration of Raney's algorithm other than the first, the effect of the first iteration of the output phase is to output a symbol coinciding with the last input, and replace M by a column-balanced matrix. Subsequent iterations replace M by the next matrix in the unique column-sequence to which M belongs, so that on termination of the output phase $M \in DB$.

In view of the exceptional nature of the first complete iteration, it will be convenient in the sequel to regard the first complete iteration together with the output phase of the second complete iteration as a preprocessing step which transforms the computation of $M[x]$ where $M \in P$ and $x \in R^\infty$ to the computation of $D[z]$ where $D \in DB$ and $z \in R^\infty$ (compare the transformation described in Appendix 1). It is then natural to consider the following modified form of Algorithm 3.1:

Algorithm 4.2: "Raney's algorithm for double-balanced matrices"

```

< q := ualbuc... where z = [a;b;c, ...] >;
N := D; {D ∈ DB}
do true →
  {N ∈ DB}
  do N ∈ RB →
    < read s, the next symbol of p >;
    if s = 'u' → N := NU
    if s = 'l' → N := NL
  fi
  {N ∈ CB}
od;
{N ∈ P \ RB and either the last input was u and NU-1 ∈ RB
or the last input was l and NL-1 ∈ RB }
do N ∉ RB →
  if U-1N ∈ P → <output 'u'>; N := U-1N
  if L-1N ∈ P → <output 'l'>; N := L-1N
  fi
  {N ∈ CB}
od
od

```

\$5. Raney's transducers.

The results of \$4. readily show that Algorithm 4.2 implicitly contains the description of a special kind of "finite state machine". When each complete iteration is initiated N is a double-balanced matrix D ; during the input phase N is successively replaced by the next matrix in its row-sequence until on the final iteration it becomes no longer row-balanced. At this point, output is given, and N is successively replaced by the next matrix in its column-sequence until it is once more double-balanced. In the course of a particular computation using Algorithm 4.2, a complete iteration can be initiated in a finite number of states only, since $\det M = n$ is invariant, and DB_n is finite (Cor. 2.2.7 (ii)). For each double-balanced matrix D , the possible sequences of input that can be accepted in a single input phase are trivial to determine from the characterisation of the row-sequence of D given in Cor. 4.1.3, and for each such sequence the output sequence returned and the double-balanced matrix which results on output are unambiguously determined. This motivates consideration of a simple computational model of Algorithm 4.2, as it applies for fixed n :

Definition: Given n , the n -th Raney transducer $RT(n)$ is the machine having DB_n for its set of states, $A = \{u, l\}$ for its input and output alphabet, and a set of transitions consisting of quadruples (D_i, v, w, D_2) such that if a complete iteration of Algorithm 4.2 is initiated with $N = D_i$, then v is accepted in the input phase, w is returned in the output phase and $N = D_2$ on termination.

Remark: $RT(n)$ differs from a classical finite state machine in that a sequence of input symbols (rather than a single symbol) may be required to prompt a change of state, and a sequence of output symbols (rather than a single output symbol) may be returned when such a transition occurs.

Studying the structure of $RT(n)$ is essentially studying the infinite behaviour of Algorithm 4.2 for fixed n . For instance, $RT(1)$ has a single state I and transitions (I, u, u, I) and (I, l, l, I) , reflecting the fact that mutually homographically related real numbers have continued fraction expansions which agree asymptotically (see [K] p.335). For small values of $n > 1$ (as the case $n=2$ discussed below illustrates) it may be useful to precompute $RT(n)$, and thereby save the re-computation of transitions implicit in Algorithm 4.2. In general, $RT(n)$ comprises a number of disjoint components, but if n is square-free, then $RT(n)$ is connected. (See Cor. 5.1.3.) In particular, if n is prime, $RT(n)$ is connected with n states. (See Cor. 4.1.4.). Representations of $RT(2)$ (see [R] p.279), $RT(4)$ and $RT(6)$ are given in Appendix 2. Similar diagrams representing $RT(3)$, $RT(5)$ and $RT(7)$ appear in [R].

A simple inspection of $RT(2)$ justifies a prescription for transforming p in A^ω , where $E(p) = x$, to q in A^ω , where $E(q) = 2x$. Explicitly:

Let $T = \{l^2, u\}$ and $H = \{l, u^2\}$. The string p in A^ω can be uniquely parsed into the form

$$t_1 . lu . h_1 . ul . t_2 . lu . h_2 . ul \dots t_k . lu . h_k . ul \dots$$

where $t_i \in T$ and $h_i \in H$ for $i \geq 1$. The string q is then derived by transforming the segments of the parsed string p , replacing

$$\begin{aligned} \text{each } t_i(l^2, u) &\text{ by } t_i(l, u^2) \\ \text{and each } h_i(l, u^2) &\text{ by } h_i(l^2, u) \end{aligned}$$

for $i \geq 1$, and replacing each 'ul' by 'lu' and each 'lu' by 'ul'.

This is an analogue in A^ω of a prescription for computing the continued fraction expansion of $2x$ from that of x given by Hurwitz in 1891. (See [R] and [K] p.335).

The rest of this section, closely based on [R], concerns properties of $RT(n)$ significant in relation to the behaviour of Algorithm 4.2. The connectivity of $RT(n)$ determines which homographic transformations are so closely related that one can arise as an intermediate computation in the computation of another. A simple bound on the number of input symbols which can be read without input being given is also derived. (See Cor. 5.1.4.)

Theorem 5.1:

Let $M \in DB_n$, and suppose that S_1, S_2, \dots, S_t are as in Cor. 4.1.3.

If $v \in A^*$, then:

- (i) there is at most one transition of the form $(M, v, *, *)$ in $RT(n)$.
- (ii) there is a transition of the form $(M, v, *, *)$ in $RT(n)$ iff
 $v = \text{cap}^{-1}(S_1 S_2 \dots S_k) \cdot s$ where $1 \leq k \leq t$, $s = 1$ or u , and $\text{cap}(v) \notin RB$.
- (iii) (M, v, w, N) is such a transition iff
 v is as in (ii), w is of the form $s \cdot z$ and $M \cdot \text{cap}(v) = \text{cap}(w) \cdot N$.

Proof: Referring to the operational account of Algorithms 3.1 and 4.2 given in §4, it is easy to show that:

- (i) is a consequence of Prop. 3.2 (i)
- (ii) follows from Cor. 4.1.3
- (iii) follows from the fact that in any complete iteration of Algorithm 4.2 the first output and the last input coincide.

Cor. 5.1.1: There is a natural 1-1 correspondence between the set of transitions of $RT(n)$ and

- (a) the set of matrices M in P_n such that for some X in $\{L, U\}$:
 $MX^{-1} \in RB$ and $X^{-1}M \in CB$
- (b) the set of pairs (R, C) such that $R \in RB_n$ and $C \in CB_n$, and
either $L^{-1}RL = C$ or $U^{-1}RU = C$.

Proof:

- (a) $MX^{-1} \in RB$ and $X^{-1}M \in CB \iff$
 $MX^{-1} = D_1 S_1 \dots S_t$ canonically and
 $X^{-1}M = T_1 \dots T_t D_2$ canonically,
where D_1 and $D_2 \in DB$ (Cor. 2.2.5)
 $\iff M = D_1 S_1 \dots S_t X = X T_1 \dots T_t D$
 $\iff (D_1, v, w, D_2)$ is a transition in $RT(n)$,
where $v = \text{cap}^{-1}(S_1 \dots S_t X)$ and
 $w = \text{cap}^{-1}(X T_1 \dots T_t)$ (Thm. 5.1 (iii)).

- (b) If $X = L$ or U and $X^{-1}RX = C$ then $M = RX$ satisfies
 $MX^{-1} \in RB$ and $X^{-1}M \in CB$.

Conversely, if $R = MX^{-1} \in RB$ and $C = X^{-1}M \in CB$ then $X^{-1}RX = C$.

In analysing the structure of the Raney transducers, symmetry plays an essential part. Two symmetry-preserving maps $P \rightarrow P$ are of interest: transposition of matrices, and "double transposition" mapping

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ to } M^\delta = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$$

Following [R], 'rev' and 'int' are used to denote 'string reversal' and 'l-u interchange' in A^* .

Lemma 5.2:

- (i) $\left\{ \begin{array}{l} \text{Transposition} \\ \text{Double transposition} \end{array} \right\}$ is an $\left\{ \begin{array}{l} \text{anti-automorphism} \\ \text{automorphism} \end{array} \right\}$ of the monoid P_1 .
- (ii) If $v \in A^*$ and $M = \text{cap}(v)$ is in P_t , then:
 $M^\tau = \text{cap}(\text{rev}(\text{int}(v)))$ and $M^\delta = \text{cap}(\text{int}(v))$.

Proof: (i) is a simple exercise.

- (ii) follows from (i) and the fact that $U^\tau = U^\delta = L$ and $L^\tau = L^\delta = U$.

Cor. 5.1.2: If (M, v, w, N) is a transition in $RT(n)$, then
 $(N^\tau, \text{rev}(\text{int}(w)), \text{rev}(\text{int}(v)), M^\tau)$
and $(M^\delta, \text{int}(w), \text{int}(v), N^\delta)$
are also transitions.

Proof: Use Lemma 5.2 (ii) and Theorem 5.1 (iii).

Notation:

If $M \in P$, the gcd of the elements of M will be denoted by ' $\gcd(M)$ '

Cor. 5.1.3:

For each k such that k^2 divides n , the submachine of $RT(n)$ whose states are the matrices M in DB_n with $\gcd(M) = k$, together with all transitions in $RT(n)$ involving such states, forms a connected component $RT(n,k)$ of $RT(n)$ which is strongly connected and isomorphic with $RT(n/k^2, 1)$.

Proof: If $S = L$ or U then $\gcd(M) = \gcd(MS) = \gcd(SM)$ so that the gcd of the elements of the state matrix is invariant under transitions in $RT(n)$. Hence $RT(n,k)$ is a connected component of $RT(n)$ if it is connected. The map $RT(n,k) \rightarrow RT(n/k^2, 1)$ mapping

$$\begin{pmatrix} ak & bk \\ ck & dk \end{pmatrix} \text{ to } \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

respects all transitions, and hence defines an isomorphism of transducers. It thus suffices to show that for all n the transducer $RT(n, 1)$ is strongly connected.

This is simply proved in three steps:

(a) Let $C \in DB_n$ be lower-triangular, and let D be the diagonal matrix having the same diagonal entries. If $\gcd(D) = 1$, then there is a path (i.e. a sequence of transitions) from C to D in $RT(n, 1)$.

Proof of (a): Let D be the diagonal matrix $\langle g, h \rangle$. Inputting only '1' 's to C , and outputting '1' 's as appropriate, will transform the non-zero off-diagonal element c of C to any residue of the form $(kh+c) \bmod g$, but leave the diagonal elements unchanged. Since $(g, h) = 1$, there is a solution of $kh+c \equiv 0 \pmod{g}$.

(b) If D_1 and D_2 are diagonal matrices, and $\gcd(D_1) = \gcd(D_2) = 1$, then there is a path from D_1 to D_2 in $RT(n, 1)$.

Proof of (b): In view of Cor. 5.1.2, it suffices to exhibit a path from the diagonal matrix $\langle n, 1 \rangle$ to the diagonal matrix $\langle g, h \rangle$. The existence of such a path follows from the identity:

$$\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} L^{h-1} U = U L^{(h-1) \div g} \begin{pmatrix} g & 0 \\ c & h \end{pmatrix}$$

where $0 \leq c < g$, and the result of (a).

(c) if $M \in DB_n$, and $\gcd(M) = 1$, then there is a path from M to a diagonal matrix, and vice versa.

Proof of (c): In view of Cor. 5.1.2 and the fact that $M = N$ for some matrix N in $RT(n)$, it suffices to exhibit a path from M to a diagonal matrix. Let S_1, S_2, \dots, S_t be as in Cor. 4.1.3. From the identity:

$$MS_1 S_2 \dots S_t = \begin{pmatrix} C+g & B \\ C & B+g \end{pmatrix}$$

it follows that

$$MS_1 S_2 \dots S_t U = U L^{C \div g} \begin{pmatrix} g & 0 \\ c & h \end{pmatrix}$$

where $0 \leq c < h$. If $c = 0$ or $\gcd(g, h) = 1$ then the result follows from (a). If neither of these conditions holds, then the above construction gives a path from M to a matrix C such that:

$$g = \gcd(p(M), q(M)) > \gcd(p(C), q(C)) = \gcd(g-c, h)$$

(in the notation of Cor. 4.1.1) from which (c) follows by induction.

Remark: The connected component $RT(n, k)$ of $RT(n)$ is the transducer defined by Raney in [R] (p.273 Defn. 6.5).

Cor.5.1.4: If (M, v, w, N) is a transition in $RT(n)$, then both v and w have length at most n .

Proof: (i) Let $M \in DB_n$. The longest input sequence which $RT(n)$ can accept in state M without yielding an output has as many symbols as there are subtraction steps in computing $\gcd(p(M), q(M))$ using Euclid's algorithm. Let this number be K . If M is the diagonal matrix $\langle n, 1 \rangle$ then $K = n$.

Each subtraction step of Euclid's algorithm applied to $(p(M), q(M))$ properly reduces $p(M) + q(M)$. Thus $K < p(M) + q(M)$. But by Cor. 2.2.7 (i):

$$p(M) + q(M) \leq \text{tr}(M) \leq n+1.$$

\$6. Fixpoints of $R(M,)$, and the expansions of quadratic irrationals.

As Cor.'s 3.2.1 and 3.2.2 show, Raney's algorithm associates with a matrix M in P a map $A^\omega \rightarrow A^\omega$.

Definition:

Let $M \in P$.

A fixpoint of $R(M,)$ is a string f in A such that $R(M, f) = f$.

A fixpoint of $M[]$ is a real number x in R such that $M[x] = x$.

Equivalently (since $M \in P$), x is a solution of the equation:

$$c \cdot E(f)^2 + (d-a) \cdot E(f) - b = 0$$

$D(M)$ will denote the discriminant of this quadratic, viz: $(a-d)^2 + 4bc$

Lemma 6.1: Let $M \in P$. Then:

- (i) $R(M,)$ has at least one fixpoint f
and (ii) f is a fixpoint of $R(M,)$ iff $E(f)$ is a fixpoint of $M[]$.

Proof:

(ii) $R(M, f) = f$ iff $E(R(M, f)) = E(f)$ by Prop. 3.2 (iv), and Prop. 1.1.
iff $M[E(f)] = E(f)$ by Thm. 3.3

(i) follows from (ii) since it is trivial to prove that $M[]$ has at least one fixpoint in R^ω .

Notation:

P^+ will denote the subset of P consisting of matrices with non-zero entries.

Remark: If $M \in P^+$ then there is a unique fixpoint x of $M[]$ in R . Thus $R(M,)$ has at most two fixpoints if x is rational, and a unique fixpoint otherwise.

Proposition 6.2: Let $M \in P^+$, and suppose that p is an arbitrary string in A^ω . Define a sequence of elements of A :

$$p_0 = p, p_1, p_2, \dots, p_k, \dots$$

by setting $p_{i+1} = M[p_i]$ for $i \geq 0$. Then:

there is a fixpoint f of $R(M,)$ such that the length of the longest common prefix of p_i and f tends to infinity with i .

Proof: It suffices to prove that $E(p_i)$ tends to $E(f)$ as i tends to infinity. (If i is sufficiently large, there is no possibility that p_i and p_{i+1} could have large prefixes in common with two distinct encodings of a rational number $E(f)$, in view of Prop. 3.2 and Prop 1.1.)

The principle used in the proof is similar to the "power method" for computing the largest eigenvalue of a matrix. Let M be the matrix:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

The eigenvalues of M are the roots of:

$$z^2 - (a+d)z + (ad-bc) = 0$$

which are not equal in modulus since $a+d$ and $ad-bc$ are both positive. Accordingly, if a sequence of vectors (x_i, y_i) is defined by:

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = M^i \begin{pmatrix} E(p) \\ 1 \end{pmatrix}$$

then the limiting direction of (x_i, y_i) is that of the eigenvector (X, Y) of M associated with the eigenvalue of larger modulus. Since, for all N in P and real numbers v_1, v_2, w_1 and w_2 :

$$N \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \Rightarrow N \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}$$

the limiting value of $M^i[E(p)]$ is X/Y . Moreover, X/Y (being an eigenvector) is a fixpoint of $M[]$. But $E(p_i) = E((R(M,))^i p) = M^i[E(p)]$ by Theorem 3.3, since for any matrices K and L in P and x in R^ω :

$$K[L[x]] = (KL)[x].$$

Algorithm 6.3:

```

M := M0; {M0 ∈ P+}
do true →
  { (cap(out))-1 · M0 · cap(out) = M }
  if U-1MU ∈ P → <output 'u'>; M := U-1MU
  [] L-1ML ∈ P → <output 'l'>; M := L-1ML
fi
od

```

Justification: The algorithm is essentially derivable as a particular "mode of execution" of Algorithm 3.4. The principle is to execute Algorithm 3.4 with an input sequence determined "at run-time", and contrived to ensure that input and output sequences are the same. The execution sequence is such that input is accepted on the odd-numbered iterations of the do ... od clause, and output is given on the even-numbered iterations. On an input iteration, the chosen input is 'u' if $U^{-1}MU \in P$ and 'l' if $L^{-1}ML \in P$ (see Prop. 4.1). (There is here an element of non-determinacy as both $U^{-1}MU$ and $L^{-1}ML$ may (exceptionally) be in P). On the succeeding iteration the output given coincides with the last input, so that the combined effect of a consecutive pair of iterations of Algorithm 3.4 in this mode of execution is precisely that of a single iteration of the do true → ... od clause of Algorithm 6.3. The correctness of Algorithm 6.3 follows from Cor. 3.5.1.

Remark: The correctness of Algorithm 6.3 guarantees that the only non-determinacy that can occur is concerned with the choice between the suffices " lu^∞ " and " ul^∞ " when $E(f)$ is rational.

An alternative justification of Algorithm 6.3 analogous to the justification of Algorithm 3.1 in §3 is possible. Algorithm 6.3 computes the element(s) of A which has(ve) the recursive definition:

```

fx(p) = if U-1MU ∈ P → u. fx(U-1MU)
        [] L-1ML ∈ P → l. fx(L-1ML)
        fi

```

The solution(s) of this equation is(are) the encoding(s) of the unique positive real number $e(M)$ satisfying:

```

e(M) = if U-1MU ∈ P → 1 + e(U-1MU)
        [] L-1ML ∈ P → 1/(1 + 1/e(L-1ML))
        fi

```

The observation that:

```

L-1ML[x] = x <=> M[x/(1+x)] = x/(1+x)
and U-1MU[x] = x <=> M[1+x] = 1+x

```

(the analogue of Proposition 2.1) then establishes that $e(M)$ is a fixpoint of $M[\]$.

Remark: The use of the "if ... [] ... fi" notation above reflects the non-deterministic nature of the definition of $fx(M)$. In this context, an "if ... then ... else ... fi" construct would be inadequate.

Notation:

If $w \in A^*$, then $\langle w \rangle$ will denote the string $w_1 w_2 \dots w_k \dots$ in A^ω where $w_i = w$ for $i > 1$.

The subset of P (resp. P_n) consisting of matrices M such that $D(M)$ is not a perfect square will be denoted by Q (resp. Q_n). Note that Q is a subset of P^+ .

Theorem 6.4: Suppose that $M_0 \in Q$ and that f is a fixpoint of $R(M_0,)$ such that $E(f)$ is irrational. Then

- (i) the subset of P_1 consisting of matrices commuting with M_0 is the submonoid generated by a single matrix $W = W(M_0)$.
and (ii) if $w = \text{cap}^{-1}(W)$, then w belongs to $A^* \setminus (u^* \cup 1^*)$ and is the shortest string such that $f = \langle w \rangle$. In particular, f has a purely periodic encoding.

Proof: It will be convenient to prove (i) and (ii) in parallel.

Let f be computed using Algorithm 6.3. The assignments $M := L^{-1}ML$ and $U := U^{-1}MU$ leave $\det M$, $\text{tr}(M)$ and $D(M) = \text{tr}(M)^2 - 4(\det M)$ invariant. Moreover, the set S of matrices M in P_n with trace t and discriminant D is finite, provided that D is not a perfect square. Explicitly:

$$\text{if } M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ then } a+d=t \text{ and } 0 < bc = ad-n \leq t^2/4 - n$$

This proves that f is ultimately periodic, but more is true.

Consider an arbitrary matrix M in S . In the computation of $\text{fx}(M)$ using Algorithm 6.3, there can be no non-determinacy since the fixpoint of $M[]$ is irrational. Hence one and only one of $L^{-1}ML$ and $U^{-1}MU$ is in S . Now $M \in S$ iff $M^T \in S$, whence:

$$\begin{aligned} U^{-1}MU \in S &\Leftrightarrow (U^{-1}MU)^T \in S \\ &\Leftrightarrow (U^{-1})^T M^T U^T \in S \\ &\Leftrightarrow L^{-1}M^T L \in S \end{aligned}$$

Similarly $L^{-1}ML \in S \Leftrightarrow U^{-1}MU \in S$.

These results show that one and only one of $U^{-1}MU$ and $L^{-1}ML$ is in S , from which it follows that the sequence of conjugations of the matrix M_0 initiated by Algorithm 6.3, being ultimately periodic, must eventually lead to $M = LM_0L^{-1}$ or UM_0U^{-1} (whichever is in S) and thence to $M = M_0$. If w is the sequence of outputs given prior to the second occasion on which $M = M_0$, then $f = \langle w \rangle$, and w contains at least one '1' and at least one 'u' since $E(f)$ is irrational. Moreover, if $W = \text{cap}(w)$, then $W^{-1}M_0W = M_0$ in view of the loop invariant in Algorithm 6.3, so that all powers of W commute with M_0 .

To show that w is the shortest string in A^* such that $f = \langle w \rangle$, suppose that w is of the form z^k where $z \in A^*$ and z is a prefix of w . If $Z = \text{cap}(z)$, and the execution of Algorithm 6.3 as described above is suspended after z has been output, then $M = Z^{-1}M_0Z = N$, say. From the definition of w it is evident that $f = \langle z \rangle = \langle w \rangle$ is a fixpoint of both $N_0[]$ and $M_0[]$.

Let $N_0 = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ and $M_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where p, q, r, s and $a, b, c, d > 0$.

(Both N and M are in Q .) Since $N[]$ and $M[]$ have a common fixpoint:

$$(p - s + \sqrt{D})/2r = (a - d + \sqrt{D})/2c,$$

whence $c = r$ and $p-s = a-d$ as \sqrt{D} is irrational. But

$$\text{tr}(N_0) = p+s = \text{tr}(M_0) = a+d,$$

so that $p = a$ and $s = d$, and

$$\det N = ps - rq = \det M = ad - bc,$$

so that $b = q$. By definition of w , it follows that $z = w$ and $k = 1$.

Now suppose that $V^{-1}M_0V = M_0$ where $V = \text{cap}(v)$ and v is a string of length t in A^* . Since $M_0V = VM_0$, Algorithm 3.4, initiated with $p = \langle v \rangle$ and $M = M_0$, can be repeatedly executed in such a way that v is first input symbol by symbol in t successive iterations, and then output symbol by symbol in t successive iterations. By Cor. 3.5.1, $\langle v \rangle = f$, the fixpoint of M_0 , and v is a prefix of $\langle w \rangle$. But this entails $v = w$ and $V = W$, since w has minimal length subject to $f = \langle w \rangle$.

Notation:

If $M \in Q$, then:

$f(M)$ will denote the fixpoint of $R(M,)$,
 $w(M)$ the element of $A^* \setminus (u^* \cup l^*)$ defined in Thm.6.4 (i),
 and $W(M) = \text{cap}(w(M))$, the matrix in Thm.6.4 (ii).

Cor. 5.4.1:

- (i) $P_i \setminus Q_i$ is the set of powers of L and U .
 Equivalently, Q_i is the set of matrices of trace > 2 in P_i .
- (ii) If $N \in Q$, then $W(N) \in Q_i$, $f(N) = f(W(N))$, and $W(W(N)) = W(N)$.
- (iii) If $N \in Q_i$, then $W(N) = N$.

Proof:

(i) If $M \in P_i$, then $D(M) = \sqrt{(\text{tr}(M))^2 - 4 \cdot \det M} = \sqrt{(\text{tr}(M))^2 - 4}$. Thus $D(M)$ is rational iff $\text{tr}(M) = 2$, in which case the diagonal elements of M are both 1, and one or other of the off-diagonal elements is 0.

(ii) $W(N)$ is in Q , in view of (i). Since each matrix in Q has a unique fixpoint in R^∞ :

$$x \in R^\infty \text{ and } Nx = x \Rightarrow Wx = WNx = NWx \Rightarrow Wx = x.$$

Thus W and N have a common irrational fixpoint, and $f(N) = f(W(N))$, by Prop.1.1 (ii).

Suppose that $M = \text{cap}(v.s)$, where $s \in A$ and $v \in A^*$. If $S = \text{cap}(s)$, then $S^{-1}MS = \text{cap}(s.v) \in P$. Hence Algorithm 6.3, applied to $M_0 = \text{cap}(z)$ in Q_i , successively transforms M to $\text{cap}(z_0), \text{cap}(z_1), \dots, \text{cap}(z_k)$ where $z_0 = z_k = z$ and z_{i+1} is obtained from z_i by applying a cyclic permutation. As in the proof of Thm. 6.4 (i), M will be first restored to M_0 after the shortest string w such that $\langle w \rangle = \langle z \rangle$ has been output. If $M_0 = W(N)$, where N is in Q , then $z = w(M_0)$, and so $w = z$ by Theorem 6.4 (ii).

(iii) is implicit in the proof of (ii).

Given M in Q , the matrix $W(M)$ can be computed by the following modified form of Algorithm 6.3, which is implicitly justified in the proof of Thm.6.4 (i).

Algorithm 6.5:

```

M := M0; {M0 ∈ Q}
if U-1MU ∈ P → W := U; M := U-1MU
if L-1ML ∈ P → W := L; M := L-1ML
fi;
do M ≠ M0 →
  { (cap(out))-1 · M0 · cap(out) = M }
  if U-1MU ∈ P → W := W.U; M := U-1MU
  if L-1ML ∈ P → W := W.L; M := L-1ML
fi
od;
<output the matrix W>

```

Cor. 5.4.2: Let $N \in Q_i$, and let r and s be non-negative integers, not both zero. If a sequence of vectors is defined by:

$$N^i \begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} r_i \\ s_i \end{pmatrix}$$

then $r_i \leq r_{i+1}$, $s_i \leq s_{i+1}$ and $r_i + s_i < r_{i+1} + s_{i+1}$ for $i \geq 0$.

Proof:

Let $N = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$. Then $N \begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} xr+ys \\ zr+ts \end{pmatrix}$.

Since x, y, z and t are positive, it follows that $xr+ys \geq r$ and $ys+zs \geq s$. Moreover:

$$xr+ys+zs+ts = (xr+ts) + (ys+zs) > r+s \text{ since } xr+ts \geq r+s \text{ and } ys+zs > 0.$$

Cor. 6.4.3: Let x be a positive irrational. The following conditions on x are equivalent:

- (a) $x = E(f(M))$ for some M in Q .
- (b) $x = E(f(M))$ for some M in Q_+ .
- (c) x has a purely periodic encoding in A^∞ .
- (d) x is a quadratic irrational whose algebraic conjugate \bar{x} is negative.

Proof:

(a) \Rightarrow (b) in view of Cor. 6.4.2 (ii), and (b) \Rightarrow (a) is trivial.

(a) \Rightarrow (c) by Thm. 6.4 (i)

(c) \Rightarrow (d) Suppose that $x = E(\langle v \rangle)$ where $v \in A^*$, and v is a minimal period for $\langle v \rangle$. If $V = \text{cap}(v)$, then $w(V) = v$ by Cor. 6.4.1 (iii).

(a) \Rightarrow (d):

Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $D(M)$ exceeds $a-d$ in modulus, as M is in Q . Thus:

the quadratic equation $M[z] = z$ has a negative root, the conjugate of x .

(d) \Rightarrow (a):

From (a), x is a root of a quadratic equation:

$$Ax^2 + Bx - C = 0$$

where A, B and C are integers, and A and C are positive. Thus:

$$M = \begin{pmatrix} T & C \\ A & T+B \end{pmatrix}$$

is in P for suitably chosen $T > 0$, and $x = E(f(M))$.

Cor. 6.4.4: The positive irrational x satisfies the equivalent conditions of Cor. 6.4.3 iff for some $k \geq 2$, $a_k \geq 0$ and $a_i > 0$ for $i=0, 1, \dots, k-1$:

$$\begin{aligned} x(\geq 1) &= [a_0; a_1, \dots, a_{k-1}, a_k + a_0, a_1, \dots, a_k + a_0, a_1, \dots] \\ \text{or } x(< 1) &= [0; a_0, a_1, \dots, a_{k-1}, a_k + a_0, a_1, \dots, a_{k-1} + a_0, a_1, \dots] \end{aligned}$$

Proof: Take $x = E(\langle v \rangle)$ in condition (c) of Cor. 6.4.3, where

$$v = u^{a_0} 1^{a_1} \dots 1^{a_{k-1}} u^{a_k} \text{ or } 1^{a_0} u^{a_1} \dots u^{a_{k-1}} 1^{a_k}$$

Cor. 6.4.5: (Lagrange 1770)

Every positive quadratic irrational has an ultimately periodic continued fraction expansion.

Proof: y can be expressed as $m + r/s + x$ where m, r, s are non-negative integers and $s > r$, and x is a quadratic irrational satisfying the equivalent conditions of Cor. 6.4.3. Computing $(sx + r)/s$ by Algorithm 4.2 must lead to an ultimately periodic output since x is purely periodic and DB_{s^2} is finite.

Cor. 6.4.6: Let $M \in Q$. Then $(W(M))^\tau = W(M^\tau)$ and $(W(M))^\delta = W(M^\delta)$.

Proof: If $X \in P$, then $MX = XM$ iff $X^\tau M^\tau = M^\tau X^\tau$ by Lemma 5.2, and thus $(W(M))^\tau = W(M^\tau)$ by Thm. 6.4. The proof for δ is similar.

Cor 6.4.7: Let $x = E(\langle v \rangle)$ be a positive quadratic irrational with a negative algebraic conjugate \bar{x} . Then $(-1/\bar{x})$ has the encoding $\langle w \rangle$ in A^∞ , where $w = \text{rev}(\text{int}(v))$.

Proof: Let $x = E(f(M))$ where $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in P_+$.

Then $cx^2 + (d-a)x - b = 0$, whence $y = (-1/\bar{x}) > 0$ satisfies the equation:

$$by^2 + (d-a)y - c = 0.$$

Hence $y = E(f(M^\tau))$. Thus $y = w(M^\tau) = \langle \text{cap}^{-1}(\text{cap}(v))^\tau \rangle = \text{rev}(\text{int}(v))$, by Lemma 5.2, and Cor. 6.4.6.

Cor. 5.4.8: (Galois 1828)

Let x be a positive quadratic irrational.

The continued fraction expansion of x is purely periodic iff
 $x > 1$ and $-1 < \bar{x} < 0$.

Proof: Since either of the stated conditions ensures that the equivalent conditions of Cor. 6.4.3 are satisfied:

x has a purely periodic continued fraction expansion

$\Leftrightarrow x = [a_0; a_1, \dots, a_{k-1}, a_k + a_0, a_1, \dots] \text{ and } a_k = 0 \text{ (Cor. 6.4.4).}$

$\Leftrightarrow x$ has the encoding $\langle v \rangle$ where $v = u^{a_0} \dots 1^{a_{k-1}}$

$\Leftrightarrow x > 1$ and $(-1/\bar{x}) > 1$ by Cor. 6.4.7.

Cor. 5.4.9:

Let $M \in Q$, and let $x = E(f(M))$. Then

(i) $M = M^{\delta\tau} \Leftrightarrow x = \sqrt{b/c}$ for positive integers b and c

$\Leftrightarrow x + \bar{x} = 0$

$\Leftrightarrow w(M) = \text{rev}(w(M))$

(ii) $M = M^{\tau} \Leftrightarrow x = (\pm m + \sqrt{m^2 + 4n^2})/2n$ for positive integers m and n

$\Leftrightarrow x \cdot \bar{x} = (-1)$

$\Leftrightarrow w(M) = \text{rev}(\text{int}(w(M)))$

Proof:

Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then:

(i) $M = M^{\delta\tau} \Leftrightarrow a = d$

$\Leftrightarrow x = \sqrt{b/c}$

$\Leftrightarrow x + \bar{x} = a - d = 0$

$\Leftrightarrow W(M) = (W(M))^{\delta\tau}$ by Cor. 6.4.1 (ii) and Cor. 6.4.7

$\Leftrightarrow w(M) = \text{rev}(w(M))$ by Lemma 5.2

(ii) $M = M^{\tau} \Leftrightarrow b = c$

$\Leftrightarrow x = (\pm m + \sqrt{m^2 + 4n^2})/2n$ where $m = |a-d|$ and $n = c$

$\Leftrightarrow x\bar{x} = (-b/c) = (-1)$

$\Leftrightarrow W(M) = W(M)^{\tau}$ by Cor. 6.4.1 (ii) and Cor. 6.4.7

$\Leftrightarrow w(M) = \text{rev}(\text{int}(w(M)))$ by Lemma 5.2.

Remark: The results of this section may be helpful in understanding the structure of Raney transducers (see §5).

Let M be in DB_n , and suppose that $M[\]$ has an irrational fixpoint. The transducer $RT(n)$, when initially in state M , responds to the input sequence $w(M)$ by outputting $w(M)$ whilst cycling through a sequence of distinct states and returning to the state M . The correspondence between states of $RT(n)$ and 'cycles of states' generated in this way is intriguing in that it suggests connections between the structure of $RT(n)$ and encodings of quadratic irrationals with various different discriminants. This is of particular interest if $n=p$ is prime, when only three of the p matrices in DB_n have rational fixpoints, namely:

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} (p+1)/2 & (p-1)/2 \\ (p-1)/2 & (p+1)/2 \end{pmatrix}$$

(If M has a rational fixpoint, then $(\text{tr}(M))^2 - 4p$ is a perfect square, and $\text{tr}(M) = p+1$. This establishes that M is one of the three matrices above.) Some illustrative examples are given in Appendix 2.

\$7. Pell's equation and the parity of palindromic encodings.

Proposition 7.1:

If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Q$ and $X = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in P_1$, then:

(i) X and M commute iff

$$bz = cy \quad \dots\dots\dots (A)$$

$$\text{and } b(x-t) = (a-d)y \quad \dots\dots\dots (B)$$

(ii) (A) and (B) together imply

$$c(x-t) = (a-d)z \quad \dots\dots\dots (C)$$

$$cx^2 - (a-d)xz - bz^2 = c \quad \dots\dots (P)$$

and 3 similar quadratic identities involving the pairs of variables:

$$(x,y), (y,t) \text{ and } (z,t)$$

generated by transposition and double transposition from the relation:

$$XM = MX.$$

Proof: (i) $XM = MX$ iff (A), (B) and (C) hold by a simple calculation. Since $M \in Q$, bc is non-zero, and thus:

$$(A) \text{ and } (B) \Rightarrow bc(x-t) = (a-d)cy = (a-d)bz \Rightarrow c(x-t) = (a-d)z$$

$$\begin{aligned} (ii) \quad cx^2 - (a-d)xz - bz^2 &= x(c(x-t) - (a-d)z) + cxt - bz^2 \\ &= c(xt - yz) \text{ by (C) and (A)} \\ &= c \text{ since } X \in P_1. \end{aligned}$$

By Lemma 5.2,

M and X commute iff M^τ (resp. M^δ) and X^τ (resp. X^δ) commute.

Hence the 3 equations derived from (P) by applying the permutations:

$$(a \ d) (x \ t), (a \ d) (x \ t) (b \ c) (y \ z) \text{ and } (b \ c) (y \ z)$$

of a, b, c, d, x, y, z, t are all equivalent to (P).

Cor. 7.1.1: Let M be as in Prop. 7.1, and let $W = W(M)$. Then:

(i) there are infinitely many solutions of the equations (A) and (B), given by taking $X = W^i$ for $i \geq 0$

(ii) there are infinitely many solutions of the equation (P), given by:

$$\begin{pmatrix} x \\ z \end{pmatrix} = W^i \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Proof: The result follows from Thm. 6.4 and Prop. 7.1. The solutions are distinct by Cor. 6.4.2.

Remark: Algorithm 6.5 provides a simple method of computing solutions for (A) and (B), and for (P).

In the context of Prop. 7.1, the special case $M = M^{\delta\tau}$ is of interest. Under this hypothesis, equation (P) reduces to the form:

$$cx^2 - bz^2 = c$$

which in the particular case $c=1, b=n$ (when $E(f(M)) = \sqrt{n}$) is the classical "Pell's equation" (see [D]).

Cor. 7.1.2: Let M and X be as in Prop. 7.1, but subject to the additional condition $a = d$. Then

$$(i) \quad XM = MX \Leftrightarrow bz = cy \text{ and } x = t$$

$$(ii) \quad XM = MX \Rightarrow cx^2 - bz^2 = c \quad \dots\dots\dots (P^*)$$

(iii) if x and z are non-negative integers satisfying (P^*) , then there are non-negative integers y and t such that X and M commute.

Proof: (i) and (ii) Under the hypothesis $a = d$, the equation (B) of Prop. 7.1 reduces to " $x=t$ ", and (P) reduces to (P^*) .

(iii) Let x and z satisfy (P^*) . If $g = \gcd(b, c)$ and $\bar{c} = c/g, \bar{b} = b/g$ then $\bar{c}x^2 - \bar{b}z^2 = \bar{c}$ where $\gcd(\bar{b}, \bar{c}) = 1$. Thus $z = k\bar{c}$ where k is a non-negative integer, and $y = (\bar{b}z)/\bar{c}$ is a non-negative integer such that $bz = cy$. Thus, choosing $t = x$ ensures that X commutes with M , and that $\det X = 1$, since $x^2 - (bk)(kc) = x^2 - yz = 1$.

Cor. 7.1.3:

If $M = \begin{pmatrix} a & b \\ c & a \end{pmatrix} \in Q$ and $W = W(M) = \begin{pmatrix} x & y \\ z & x \end{pmatrix}$ then:

(x, z) is the least solution of (P^*) in positive integers, and $y = (bz)/c$.

Proof: Let (X, Z) be any solution of (P^*) in positive integers. In view of Cor. 7.1.2 (iii) there are suitable integers Y and T such that

$$\begin{pmatrix} X & Y \\ Z & T \end{pmatrix}$$

is in P and commutes with M . But then $X \geq x$ and $Z \geq z$, by Thm. 6.4 and Cor. 6.4.2.

Remark: Under the general conditions of Prop. 7.1, a solution of (P) is not necessarily associated with a matrix in P which commutes with M . For instance, if $a = d+5$, $b = 1$, and $c = 2$ then $x = 3$ and $z = 1$ satisfies (P) , but $cy = bz$ has no solution. In view of Cor. 7.1.3, Algorithm 6.5 can be used to compute all solutions of (P) if $a = d$, but only determines a proper subset of all solutions in the general case.

Let M be as in Cor. 7.1.3. The string $w(M)$ in A^* is then the purely periodic part of the encoding of $\sqrt{b/c}$. By Cor. 6.4.9, w is palindromic, and accordingly:

either w is of even length and $w = v.\text{rev}(v)$ where $v \in A^*$

or w is of odd length, and $w = v.(u \text{ or } 1).\text{rev}(v)$ where $v \in A^*$.

(In the latter case $w(M)$ will be called an odd- u (resp. odd-1) palindrome.)

Finding conditions on b and c which ensure that $w(M)$ is of a particular form is closely connected with questions concerning the form of the continued fraction expansion of $\sqrt{b/c}$. (c.f. [D] p.106-110.) Since this correspondence between the classical continued fraction expansion of $\sqrt{b/c}$ and its $\{u, 1\}$ -encoding is rather confusing, it will be illustrated by example. Without essential loss of generality the case $c=1$ is considered.

By non-standard convention (compare for example [CH] p.479-480, and [D] p.103-109), the continued fraction expansion of \sqrt{n} is assigned a parity according to the numerical length of its numerical period. For instance:

$$\sqrt{21} = [4; 1, 1, 2, 1, 1, 8, \dots]$$

has an even number of quotients in its period, whilst:

$$\sqrt{29} = [5; 2, 1, 1, 2, 10, \dots]$$

has an odd number. This parity has number-theoretic significance, in that:

$$x^2 - 29y^2 = (-1)$$

has an integral solution, whilst:

$$x^2 - 21y^2 = (-1)$$

does not. $\sqrt{21}$ has the encoding $\langle u^4 1 u^2 u^1 u^4 \rangle$, whilst that of $\sqrt{29}$ is:

$$\langle u^5 1^2 u^1 u^1 u^2 1 u^2 u^5 \rangle.$$

Both encodings thus correspond to palindromes of even length, but that of $\sqrt{29}$ is distinguished from $\sqrt{21}$ in that it has the form $v.\text{rev}(v)$ where in addition $v = \text{rev}(\text{int}(v))$.

Where the $\{u, 1\}$ -encoding is concerned, it is also natural to explore the distinction between radicals associated with even palindromic periods and odd- u and odd-1 palindromic periods. Examples of such are:

$$\sqrt{19} = [4; 2, 1, 3, 1, 2, 8, \dots]$$

with the odd-1 palindromic encoding $\langle u^4 1^2 u^3 u^1 u^2 u^4 \rangle$, and

$$\sqrt{23} = [4; 1, 3, 1, 8, \dots]$$

with an odd- u palindromic encoding.

The parity of the encoding of $\sqrt{b/c}$ can often be simply determined from the residue of bc modulo 4, as Proposition 7.2 and its corollaries show. Further necessary and sufficient conditions for $\sqrt{b/c}$ to have a palindromic encoding of each of the types cited above are explored in §8 and §9. These conditions are potentially of more number-theoretic interest, and take the form of assertions about the existence of solutions to Diophantine equations closely related to Pell's equation (generally subject to constraints). The classical condition for n to have a numerical period of odd length (c.f. $\sqrt{29}$ above) appears as a special case (see Cor. 8.1.5).

Proposition 7.2: Let $W \in P_1$, and let $w = \text{cap}^{-1}(W) \in A^*$. Then:

- (i) there is a surjective monoid homomorphism $\text{par}: P_1 \rightarrow \text{SL}(2, \mathbb{Z}_2)$, where the entries of $\text{par}(W)$ are the corresponding entries of W reduced modulo 2.
- (ii) $\text{SL}(2, \mathbb{Z}_2)$ is generated by $\text{par}(U)$ and $\text{par}(L)$ subject to the relations $(\text{par}(U))^2 = (\text{par}(L))^2 = (\text{par}(U)\text{par}(L))^3 = 1$, and is hence isomorphic to the symmetric group S_3 .
- (iii) w has even length iff $\text{par}(W) = I$, $\text{par}(UL)$ or $\text{par}(LU)$
iff $\text{par}(W)$ corresponds to an even permutation under the isomorphism described in (ii)

Proof: (i) is simply verified by direct computation.

(ii) It is easy to verify the stated relations between $\text{par}(U)$ and $\text{par}(L)$, and the required isomorphism follows from the fact that:

$I, \text{par}(U), \text{par}(L), \text{par}(UL), \text{par}(LU)$ and $\text{par}(ULU)$ are distinct elements of $\text{SL}(2, \mathbb{Z}_2)$.

(iii) follows from the fact that $\text{par}(U)$ and $\text{par}(L)$ correspond to transpositions under the isomorphism in (ii), so that w has even length iff $\text{par}(W)$ corresponds to an even permutation.

Cor. 7.2.1: Let b and c be positive integers, not both even, and suppose that M and W are as in Cor. 7.1.3. Then:

$w(M)$ has odd length $\Leftrightarrow (bc = 0(4) \text{ or } bc = 3(4))$ and (y or z is odd)

Proof:

\Leftarrow : Suppose that y or z is odd.

If $bc = 3(4)$, then $y = (b/c)z$ ensures that y and z are both odd. Since $cx^2 - bz^2 = c$

and b and z are odd, x is necessarily even. Thus $\text{par}(W) = \text{par}(ULU)$, and $w(M)$ has odd length by Prop. 7.2.

If $bc = 0(4)$, then $bz = cy$ ensures that y and z have opposite parity, since b and c are not both even. But then $\text{par}(W) = \text{par}(U)$ or $\text{par}(L)$ necessarily, so that $w(M)$ has odd length.

\Rightarrow : Suppose that $w(M)$ has odd length. There are three cases:

Case 1: $\text{par}(W) = \text{par}(U)$

Here x and y are odd and z is even, whence $cy = bz$ entails c even and b odd. But then $bx^2 - cy^2 = b(4)$, so that $cy = 0(4)$ and $c = 0(4)$.

Case 2: $\text{par}(W) = \text{par}(L)$

An analogue of the argument in Case 1 applies.

Case 3: $\text{par}(W) = \text{par}(ULU)$

Here x is even, y and z are both odd, and $cx^2 - bz^2 = c$ and $cy = bz$ can be satisfied only if b and c are both odd, and $-b = c(4)$. Thus $bc = 3(4)$, and y and z are odd.

Cor. 7.2.2: Let b and c be positive integers, not both even.

(i) If $bc = 1, 2(4)$ then the encodings of \sqrt{bc} and $\sqrt{b/c}$ have the same parity.

(ii) If $bc = 0, 3(4)$, b and c are coprime and b or c is square-free, then \sqrt{bc} and $\sqrt{b/c}$ have the same parity.

Proof: Let $N = \begin{pmatrix} a & bc \\ 1 & a \end{pmatrix}$ and let M and $W(M)$ be as in Cor. 7.2.1.

Then \sqrt{bc} has the encoding $\langle w(N) \rangle$, and $\sqrt{b/c}$ the encoding $\langle w(M) \rangle$. These encodings trivially have the same parity if $bc = 1, 2(4)$ by Cor. 7.2.1.

Suppose then that $bc = 0, 3(4)$, and assume (without loss of generality), that c is square-free. (The encodings of $\sqrt{b/c}$ and $\sqrt{c/b}$ have the same parity by Cor. 1.1.1). By Cor. 7.1.3, x and z are the smallest positive integers satisfying (P^*) , and since c and b are coprime, and c is square-free, c divides z . But then $x^2 - bc(z/c)^2 = 1$, and $(x, z/c)$ is the smallest solution of the classical Pell equation $X^2 - bcZ^2 = 1$.

Let $Z = z/c$ and $Y = bcZ = bz$. If c is odd, then $Y = cy = y(2)$, and $Z = z/c = z(2)$, whilst if c is even, then b is odd and $y = bZ = Z(2)$ and $z = Y/b = Y(2)$. The result then follows from Cor.'s 7.1.3 and 7.2.1.

\$8. Even palindromic encodings.

Proposition 8.1: Let $M = \begin{pmatrix} a & b \\ c & a \end{pmatrix} \in Q$. Then:

- (i) $w(M)$ has even length iff there are positive integers B, C, Z and T such that:
 - (a) $BC = bc$ and $B \neq c$
 - (b) $BT^2 - CZ^2 = c$
 - and (c) c divides both BT and CZ .
- (ii) if $w(M)$ has even length, then there is a unique pair of integers (B, C) for which (a), (b) and (c) can hold, and an associated infinite family of pairs (Z, T) satisfying (b) and (c).
- (iii) if $w(M)$ has even length, (B, C) is the unique pair of integers specified in (ii) and Z and T are minimal subject to conditions (a), (b) and (c), then $W = W(M) = V_i \cdot V_i^{st}$ where:

$$V_i = \begin{pmatrix} BT/c & CZ/c \\ Z & T \end{pmatrix}$$

and the general solution of (b) and (c) takes the form:

$$(Z_i, T_i) = (0, 1) \cdot W^i V \text{ with } i \geq 0.$$

Proof: Using Lemma 5.2, a necessary and sufficient condition for $w(M)$ to have even length is that W should factorise as a product $V \cdot V^{st}$ where V is in P_1 . Accordingly, suppose that:

$$V = \begin{pmatrix} X & Y \\ Z & T \end{pmatrix} \in P_1.$$

$V \cdot V^{st}$ commutes with M iff $V \cdot V^{st} = W^i$ some i , by Thm.6.4
 iff $bZT = cXY$ and X, Y, Z and $T > 0$ by Cor.7.1.2

Note that a necessary condition for $bZT = cXY$ is that:

$$Z(bT^2 - cY^2) = cXYT - cY^2Z = cY(XT - YZ) = cY$$

so that Z divides cY . The condition T divides cX is likewise necessary.

Supposing then that $cX = BT$ and $cY = CZ$, it may be seen that

$$bZT = cXY \text{ and } XT - YZ = 1$$

are respectively equivalent to the conditions:

$$bc = BC \text{ and } BT^2 - CZ^2 = c.$$

Thus $V \cdot V^{st}$ and M commute iff

there are positive integers B, C, Z and T such that
 $BC = bc$ and $BT^2 - CZ^2 = c$, where $cX = BT$ and $cY = CZ$.

Moreover, there exists a V in P such that $V \cdot V^{st} = W^i$ for some i iff

there are positive integers B, C, Z and T such that
 $BC = bc$ and conditions (b) and (c) in (i) hold.

Now $w(M)$ is of even length provided that there is a factorisation of W^i with i odd. To impose this extra condition on i , it suffices to ensure that V is not itself a power of W , that is (Thm.6.4), does not itself commute with M . But V commutes with M iff $bZ = cY$ and $X = T$, by Cor.7.1.2, and this can be the consistent with (b) and (c) only if $B = c$ and $C = b$.

To prove (iii) it suffices to observe that in view of the isomorphism between P_1 and Λ^* (Cor.2.2.6) there is a V in P_1 such that $V \cdot V^{st} = W^i$ with i odd if and only if there is a solution V_i for each odd i , and $V_i = W^i V_1$. In particular, by Cor.6.4.2, the smallest values of Z and T for which conditions (a), (b) and (c) are satisfied determine V_1 as explicitly described in (iii).

To prove (ii), it will suffice to show that each solution V_i with i odd is associated with the same pair of integers (B, C) . Suppose that:

$$W = \begin{pmatrix} x & y \\ z & x \end{pmatrix} \text{ and } V_i = \begin{pmatrix} X & Y \\ Z & T \end{pmatrix} \text{ where } X = BT/c \text{ and } Y = CZ/c.$$

To verify directly that $V_{i+2} = W \cdot V_i$ and V_i are associated with the same pair of positive integers (B, C) , observe that:

$$\begin{aligned} c(xX + yZ) &= xBT + bzZ \text{ since } cX = BT \text{ and } cy = bz \\ &= xBT + zBY \text{ since } BC = bc \text{ and } Y = CZ/c \\ &= B(xT + zY) \end{aligned}$$

and $c(xY + yT) = C(zX + Zz)$ similarly.

Cor. 8.1.1: Let M and W be as in Prop.8.1, and suppose that $w(M)$ has even length. If (B, C, X, Y, Z, T) is a sextuple of positive integers, and

$$V = \begin{pmatrix} X & Y \\ Z & T \end{pmatrix}$$

then the following are equivalent:

- (1) V is in P_1 and $V.V^{\delta\tau} = W^i$ for some odd i , and $B=cX/T$, $C=cY/Z$.
- (2) B, C, Z and T satisfy conditions (a), (b) and (c) of Prop.8.1(i), and $X=BT/c$, $Y=CZ/c$.
- (3) V is in P_1 , $B = c$ and $\begin{pmatrix} a & C \\ B & a \end{pmatrix} = V^{-1}MV$.

Proof:

(1) and (2) are proved equivalent in the proof of Prop.8.1.

(1) \Rightarrow (3):

From the proof of Prop.8.1 the relation $bZT = cXY$ holds, whilst

$$Z(bT^2 - cY^2) = cY = CZ$$

showing that $C = bT^2 - cY^2$. Similarly $B = cX^2 - bZ^2$. With the aid of these relations, (3) can be verified by direct computation.

(3) \Rightarrow (1):

Since $B = c$, it is evident that V and M do not commute. However, applying the anti-homomorphism $\delta\tau$ to (3) shows that:

$$M = (V^{\delta\tau})^{-1} \begin{pmatrix} a & C \\ B & a \end{pmatrix} V^{\delta\tau}$$

whence $V.V^{\delta\tau}$ commutes with M . This proves (i).

Cor. 8.1.2: If M is as in Prop.8.1, $w(M)$ has even length, and B, C, Z, T and V_1 are defined as in Prop.8.1(iii), then:

- (i) $M^{\tau} = (V_1^{\tau})^{-1} \begin{pmatrix} a & B \\ C & a \end{pmatrix} V_1^{\tau}$
- (ii) $\sqrt{B/C}$ has an even palindromic encoding with minimal period $\text{rev}(\text{int}(v_1)) \cdot \text{int}(v_1)$, where $v_1 = \text{cap}^{-1}(V_1)$.

Proof: (i) Condition (3) of Cor.8.1.1 is satisfied with $V = V_1$, and the identity in (i) is obtained directly by application of τ .

(ii) Let N denote the matrix $\begin{pmatrix} a & B \\ C & a \end{pmatrix}$.

By (i), condition (iii) of Cor.8.1.1 is satisfied with the matrix N in the role of M by the sextuple $(c, b, X=BT/c, Z, Y=CZ/c, T)$ of positive integers. By Prop.8.1(ii) and Cor.8.1.1, any sextuple satisfying condition (iii) of Cor.8.1.1 with N in the role of M is of the form (c, b, P, Q, R, S) . But such sextuples correspond one-to-one with sextuples satisfying condition (iii) of Cor.8.1.1 as stated literally for M via the correspondence:

$$(c, b, P, Q, R, S) \longleftrightarrow (B, C, P, R, Q, S)$$

given by application of the anti-isomorphism τ . Thus $W(N)$ has the factorisation $V_1^{\tau} \cdot (V_1^{\tau})^{\delta\tau} = V_1^{\tau} \cdot V_1^{\delta}$, and $\sqrt{B/C}$ has the specified encoding.

Remark: Cor.'s 8.1.1 and 8.1.2 demonstrate a reciprocal relationship between pairs (c, b) and (B, C) related as in Prop.8.1(ii) in the event that $\sqrt{b/c}$ has an even encoding. For example, let $b = 34$ and $c = 1$. Then $\sqrt{b/c}$ has the even encoding $\langle u^5 1u^2 .u^2 1u^5 \rangle$, and the appropriate values of B and C defined in Prop.8.1(ii) are $B=2$ and $C=17$. The reciprocal relationship between the pairs (c, b) and (B, C) is associated with the solubility of the equation $34T^2 - Y^2 = 17$, which is satisfied when $T = 3$ and $Y = 17$, and $\sqrt{2/17}$ has the encoding $\langle 1^2 u 1^5 .1^5 u 1^2 \rangle$.

Cor. 8.1.3: Let $M = \begin{pmatrix} a & b \\ c & a \end{pmatrix} \in Q$. Then:

- (i) $w(M)$ has even length iff there are positive integers B, C, X and Y such that:
 - (a*) $BC = bc$ and $C = b$
 - (b*) $CX^2 - BY^2 = b$
 - and (c*) b divides both CX and BY .
- (ii) if $w(M)$ has even length, then there is a unique pair of integers (B, C) , the same as that specified in Prop.8.1(ii), for which (a*), (b*) and (c*) can hold, and an associated infinite family of pairs (X, Y) satisfying (b*) and (c*).
- (iii) if $w(M)$ has even length, (B, C) is the unique pair of integers specified in (ii) and X and Y are minimal subject to conditions (a*), (b*) and (c*), then $W = w(M) = V_1 \cdot V_1^{\delta \tau}$ where:

$$V_1 = \begin{pmatrix} X & Y \\ BY/b & CX/b \end{pmatrix}$$

and the general solution of (b*) and (c*) takes the form:

$$(X_i, Y_i) = (1, 0) \cdot W^i V_1 \text{ with } i \geq 0.$$

Proof: $w(M)$ is of even length iff $w(M)^\delta = \text{int}(w(M))$ is of even length (see Lemma 5.2, Cor.6.4.6 and Cor.1.1.1), and the application of Prop.8.1 to M^δ leads to a factorisation of $W(M)^\delta = (W(M))^\delta$ as $V_1^\delta \cdot V_1^{\tau}$. Inspection of the forms of V_1 specified by Prop.8.1(iii) and Cor.8.1.3(iii) then establishes that the pairs (B, C) specified in Prop.8.1 and Cor.8.1.3(ii) coincide.

Remark: Cor.8.1.3 indicates that the asymmetry between b and c in Prop.8.1 is illusory. Cor's 8.1.4 and 8.1.5 can be dualised in a similar fashion.

Cor.8.1.4:

Let \bar{M} be as in Prop.8.1 where c is square-free. Then:

- (i) $w(M)$ has even length iff there are positive integers B, C, Z and T such that conditions (a) and (b) of Prop.8.1 are satisfied.
- and (ii) if $w(M)$ has even length then there is a unique pair of positive integers (B, C) satisfying condition (a) for which (b) can hold.

Proof: (i) If c is square-free, and $BT^2 - CZ^2 = c$ subject to $BC = bc$, then c divides $BCT^2 - (CZ)^2$, whence c divides $(CZ)^2$. But then c divides CZ , as c is square-free. Similarly, c divides BT .

(ii) is an immediate consequence of Prop.8.1 (ii), and (i).

Remark: The importance of condition (c) of Prop.8.1 in the case when c is not square-free can be illustrated by example. If $c=8$ and $b=1$ then:

$B=4$ and $C=2$ leads to a solution of (b) with $Z=T=2$

and $b/c = 1/(2\sqrt{2})$ has the odd-u encoding $\langle 1^2 u 1^2 \rangle$.

To see that Cor.8.1.4 (ii) is false in general, let $c=12$ and $b=1$. Then:

$B=2$ and $C=6$ leads to a solution of (b) with $T=9$ and $Z=5$.

In this example, $b/c = 1/(3\sqrt{2})$ has the even encoding $\langle 1^3 u^2 1^3 \rangle$, and the minimal values satisfying (a), (b) and (c) of Prop.8.1 (i) are:

$$B=3, C=4, T=4 \text{ and } Z=3.$$

Cor.8.1.4 (ii) provides a means of proving the insolubility of certain Diophantine equations. For instance, the fact that

$$2T^2 - 17Z^2 = 1 \text{ has the solution } T=3 \text{ and } Z=1$$

proves that $34T^2 - Z^2 = 1$ has no solution. (C.f. [D] p.110). This fact can also be inferred from the form of the encoding of $\sqrt{34}$, viz:

$$\langle u^5 l u^4 l u^5 \rangle$$

as the following corollary to Prop.8.1 shows:

Cor. 8.1.5: Let M be as in Prop.8.1, and let $w = w(M)$. Then:
 w can be expressed as $v \cdot \text{rev}(v)$ where $v = \text{rev}(\text{int}(v))$
 iff there are positive integers Z and T such that
 $bT^2 - cZ^2 = c$ and c divides bT .

Proof: Let V_i be the matrix defined in Prop.8.1 (iii). By Lemma 5.2

$$v = \text{rev}(\text{int}(v)) \text{ iff } V_i = V_i^T \text{ iff } c = C.$$

Hence $v = \text{rev}(\text{int}(v))$ iff (a), (b) and (c) can be satisfied subject to
 $B=b$ and $C=c$.

(An alternative proof can be obtained directly from Cor.8.1.2(ii)).

Cor. 8.1.6:

Let M be as in Prop.8.1, and let $w = w(M)$. If w can be expressed as $v \cdot \text{rev}(v)$ where $v = \text{rev}(\text{int}(v))$, then there are positive integers p, q, r and s such that $b(r^2 + s^2) = c(p^2 + q^2)$ and $ps - qr = 1$, and these conditions imply that $(pqc - rsb)^2 + (p^2c - r^2b)^2 = bc$.

Proof:

Suppose that $w = v \cdot \text{rev}(v)$, where $v = \text{rev}(\text{int}(v))$. Then v has the form $t \cdot \text{rev}(\text{int}(t))$. Let $T = \text{cap}(t)$ and $V = \text{cap}(v)$ be the matrices:

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \text{ and } \begin{pmatrix} X & Y \\ Z & T \end{pmatrix}$$

respectively. Using Cor.5.1.2, it follows that:

$$X = p^2 + q^2, Y = Z = pr + qs \text{ and } T = r^2 + s^2.$$

But $cX = bT$ by Prop.8.1.(iii), and $B=b$ by Cor.8.1.5, which proves the first part of Cor.8.1.6. Moreover:

$$\begin{aligned} (pqc - rsb)^2 + (p^2c - r^2b)^2 &= p^2c^2[p^2 + q^2] + r^2b^2[r^2 + s^2] - 2pqrsbc - 2p^2r^2bc \\ &= bc(p^2[r^2 + s^2] + r^2[p^2 + q^2] - 2pqrs - 2p^2r^2) \\ &\quad \text{using the identity proved previously} \\ &= bc, \text{ since } ps - qr = 1. \end{aligned}$$

Remark:

Cor.8.1.6 describes a method for representing appropriate integers as the sum of two squares which is closely related to a construction due to Legendre. (See [D] p.119-120).

\$9. Odd palindromic encodings.

Proposition 9.1: Let $M = \begin{pmatrix} a & b \\ c & a \end{pmatrix} \in Q$. Then:

- (i) $w(M)$ is an odd palindrome iff there are positive integers B, C, Z and T such that:
 - (a) $BC = bc$
 - (b) $BT^2 - CZ^2 = 2c$
 - (c) c divides both BT and CZ .
 - and (d) $T-Z$ and $(CZ-BT)/c$ are both even
- (ii) if $w(M)$ is an odd palindrome, then there is a unique pair of integers (B, C) for which (a) through (d) can hold, and an associated infinite family of pairs (Z, T) satisfying (b), (c) and (d). Moreover:
 - $w(M)$ is odd-u iff all solutions (Z, T) satisfy $T > Z > 0$,
 - and $w(M)$ is odd-l iff all solutions (Z, T) satisfy $Z > T > 0$.
- (iii) if $w(M)$ is an odd palindrome, (B, C) is the unique pair of integers specified in (ii) and Z and T are minimal subject to conditions (a), (b), (c) and (d), then
 - either $w(M)$ is odd-u and $W = W(M) = V_u \cdot U \cdot V_u$ where:

$$V_u = \begin{pmatrix} BT/c & (CZ-BT)/2c \\ Z & (T-Z)/2 \end{pmatrix}$$
 - or $w(M)$ is odd-l and $W = W(M) = V_l \cdot L \cdot V_l$ where:

$$V_l = \begin{pmatrix} (BT-CZ)/2c & CZ/c \\ (Z-T)/2 & T \end{pmatrix}$$
- (iv) If $w(M)$ is odd-u (resp. odd-l), and V is the matrix V_u (resp. V_l) defined in (iii), then the general solution of (b), (c) and (d) is the set of pairs (Z_i, T_i) , where $T_i = 2\bar{T}_i + Z_i$ (resp. $Z_i = 2\bar{Z}_i + T_i$) and $(Z_i, \bar{T}_i) = (0, 1) \cdot W^i V_i$ with $i \geq 0$.

Proof:

The proof is similar to that of Proposition 8.1.

Only the case when $w(M)$ is an odd-u palindrome is considered in the proof, but the generalisation to the 'odd-l' case is straightforward. The use of the substitutions $X=2\bar{X}+Y$ and $Z=2\bar{Z}+T$ in place of $Y=2\bar{Y}+X$ and $T=2\bar{T}+Z$ is the essential change required.

Using Lemma 5.2, a necessary and sufficient condition for $w(M)$ to be an odd-u palindrome is that W should factorise as a product $V \cdot U \cdot V^{\delta T}$ where V is in P_1 , and V is not a power of U . Accordingly, let:

$$V = \begin{pmatrix} X & \bar{Y} \\ Z & \bar{T} \end{pmatrix} \in P, \text{ where } X, Z \text{ and } \bar{T} > 0 \text{ and } \bar{Y} \geq 0.$$

$V \cdot U \cdot V^{\delta T}$ commutes with M iff $V \cdot U \cdot V^{\delta T} = W^i$ some i , by Thm.6.4

$$\text{iff } bZ(2\bar{T}+Z) = cX(2\bar{Y}+X) \text{ by Cor.7.1.2.}$$

Substituting $Y=2\bar{Y}+X$ and $T=2\bar{T}+Z$ in the above relation gives " $bZT=cXY$ ", whilst the condition $X\bar{T}-\bar{Y}Z=1$ transforms to $XT-YZ=2$. Now Z divides $2cY$ is a necessary condition for both $bZT=cXY$ and $XT-YZ=2$ to hold (c.f. proof of Prop.8.1), since:

$$Z(bT^2 - cY^2) = cXYT - cY^2Z = cY(XT - YZ) = 2cY$$

so that Z divides $2cY$. The condition T divides $2cX$ is likewise necessary. Supposing then that $2cX = \bar{B}T$ and $2cY = \bar{C}Z$, it may be seen that

$$bZT = cXY \text{ and } XT - YZ = 2$$

are respectively equivalent to the conditions:

$$4bc = \bar{B}\bar{C} \text{ and } \bar{B}T^2 - \bar{C}Z^2 = 4c.$$

To derive (a) and (b) it will suffice to prove that both \bar{B} and \bar{C} are necessarily even. Suppose then that \bar{C} is odd, and $\bar{B}=4k$ where $k\bar{C}=bc$. The relation $4kT^2 - CZ^2 = 4c$ entails Z even, whence $T=2\bar{T}+Z$ is even, and $X = \bar{B}T/2c = (4k/c)(T/2)$. Now observe that any factor of 2 in c divides k , since c divides $k\bar{C}$, and \bar{C} is odd. Thus X has a factor 4, and accordingly both X and Z are even, contradicting the supposition that V has determinant 1. A similar argument proves that \bar{B} cannot be odd, whence $\bar{B}=2B$, $\bar{C}=2C$ and conditions (a) and (b) hold.

The above argument proves that (a) and (b) are necessary conditions for there to exist a V such that $W = V.U.V^{\delta^T}$, for some i . To prove that (a), (b), (c), (d) subject to $T > Z > 0$ provide necessary and sufficient conditions for W to possess a factorisation as $V.U.V^{\delta^T}$ (and so complete the proof of (i), since such a factorisation is possible at all only if i is odd (compare the proof of Prop.8.1)), it is enough to show that conditions (a) through (d) together with $T > Z > 0$ guarantee that \bar{T} and \bar{Y} can be calculated as non-negative integers from T and Y .

Suppose then that (a) through (d) hold, that $T > Z > 0$ but that $CZ < BT$. (No other condition can obstruct the computation of \bar{T} and \bar{Y}). In view of (c) and the condition $T > Z > 0$, it must be that $BT \geq CZ + c$, whence:

$$BT \geq (CZ + c)(Z + 1) = CZ + (C + c)Z + c.$$

$$\begin{aligned} \text{Thus } BT^2 - CZ^2 &\geq (C + c) \cdot Z + c \\ &\geq C + 2c \text{ since } Z \geq 1 \\ &> 2c \text{ since } BC = bc \text{ is non-zero.} \end{aligned}$$

This contradicts condition (b).

For the proof of (ii), the method of proof used in Prop.8.1(ii), based on the isomorphism between P_i and A^* , applies with minor changes.

Finally, essentially as in the proof of Prop.8.1, the uniqueness of B and C follows from the observation that:

$$\begin{aligned} c(xX + yZ) &= xBT + bzZ \text{ since } cX = BT \text{ and } cy = bz \\ &= xBT + zBY \text{ since } BC = bc \text{ and } Y = CZ/c \\ &= B(xT + zY) \\ &= B(2(xT + zY) + (xZ + zX)) \end{aligned}$$

$$\text{and } c(xY + yT) = C(zX + Zz) \text{ similarly.}$$

As in the case of even palindromic encodings (c.f. Cor.8.1.3), there is complete symmetry between b and c .

Cor. 9.1.1: Let $M = \begin{pmatrix} a & b \\ c & a \end{pmatrix} \in Q$. Then:

- (i) $w(M)$ is an odd palindrome iff there are positive integers B, C, X and Y such that:
 - (a*) $BC = bc$
 - (b*) $CX^2 - BY^2 = 2b$
 - (c*) b divides both CX and BY .
 and (d*) $Y - X$ and $(CX - BY)/b$ are both even
- (ii) if $w(M)$ is an odd palindrome, then there is a unique pair of integers (B, C) , the same as that specified in Prop.9.1(ii), for which (a*) through (d*) can hold, and an associated infinite family of pairs (X, Y) satisfying (b*), (c*) and (d*). Moreover:
 - $w(M)$ is odd-u iff all solutions (X, Y) satisfy $Y > X > 0$,
 - and $w(M)$ is odd-l iff all solutions (X, Y) satisfy $X > Y > 0$.
- (iii) if $w(M)$ is an odd-u palindrome, (B, C) is the unique pair of integers specified in (ii) and X and Y are minimal subject to conditions (a*), (b*), (c*) and (d*), then
 - either $w(M)$ is odd-u and $W = W(M) = V_u \cdot U \cdot V_u$ where:

$$V_u = \begin{pmatrix} X & (Y - X)/2 \\ BY/b & (CX - BY)/2b \end{pmatrix}$$
 - or $w(M)$ is odd-l and $W = W(M) = V_l \cdot L \cdot V_l$ where:

$$V_l = \begin{pmatrix} (X - Y)/2 & Y \\ (BY - CX)/2b & CX/b \end{pmatrix}$$
- (iv) If $w(M)$ is odd-u (resp. odd-l), and V is the matrix V_u (resp. V_l) defined in (iii), then the general solution of (b*), (c*) and (d*) is the set of pairs (X_i, Y_i) , where $Y_i = 2\bar{Y}_i + X_i$ (resp. $X_i = 2\bar{X}_i + Y_i$) and $(X_i, \bar{Y}_i) = (1, 0) \cdot W^i V_i$ with $i \geq 0$.

Proof: (C.f. proof of Cor.8.1.3.) Apart from the coincidence between the pairs (B, C) specified in Prop.9.1(ii) and Cor.9.1.1(ii), the result follows directly from the application of Prop.9.1 to the matrix M^{δ} , and the observation that $w(M^{\delta})$ is odd-u iff $w(M)$ is odd-l (see Lemma 5.2, Cor.6.4.6 and Cor.1.1.1). Inspection of the expressions representing the matrix V_u or V_l in Prop.9.1 and Cor.9.1.1(iii) completes the proof.

Remark: In the context of Prop.9.1, if c is odd, then:
 (a), (b), (c) and $T-Z$ is even \Rightarrow (d).

To prove this, observe that either Z or $X = BT/c$ is necessarily odd, since $XT-YZ=1$. Since T and Z have the same parity, and c is odd, Z can only be odd. From (b), it then follows that B and C also have the same parity, and thus BT and CZ have the same parity, proving (d).

Note also that if (a) through (d) hold then:

$$T > Z \Leftrightarrow CZ \geq BT.$$

(If $CZ \geq BT$ then $T > Z$ since $BT^2 - CZ^2 > 0$, and the converse implication is explicit in the proof of Prop.9.1).

Similar observations apply in the context of Cor.9.1.1.

To simplify the discussion of odd- u and odd- l palindromic encodings as special cases of odd encodings, some notation is useful.

Let M be as in Prop.9.1, and suppose that $w(M)$ is an odd palindrome. If (B, C) is as specified in Prop.9.1(ii) and Cor.9.1.1(ii), then there are associated minimal solutions (X, Y) and (Z, T) of the equations:

$$BT^2 - CZ^2 = 2c \quad \text{and} \quad CX^2 - BY^2 = 2b$$

respectively. The notation $V(M)$ will be used to denote the matrix:

$$\begin{pmatrix} X & Y \\ Z & T \end{pmatrix}$$

Note that $V(M)$ is in P_2 . The palindrome $w(M)$ is then odd- u (resp. odd- l) if $T > Z > 0$ and $Y > X > 0$ (resp. $Z > T > 0$ and $X > Y > 0$). If $w(M)$ is odd- u (resp. odd- l), then V_u (resp. V_l) will denote the matrix:

$$\begin{pmatrix} X & \bar{Y} \\ Z & \bar{T} \end{pmatrix} \quad (\text{resp. } \begin{pmatrix} \bar{X} & Y \\ \bar{Z} & T \end{pmatrix})$$

where $\bar{Y} = (Y-X)/2$ and $\bar{T} = (T-Z)/2$ (resp. $\bar{X} = (X-Y)/2$ and $\bar{Z} = (Z-T)/2$).

The next corollaries are analogues of Cor.'s 8.1.1 and 8.1.2.

Cor. 9.1.2: Let M and W be as in Prop.9.1, and suppose that $w(M)$ is an odd- u (resp. odd- l) palindrome. If (B, C, X, Y, Z, T) is a sextuple of positive integers, such that $B=cX/T$ and $C=cY/Z$, and \bar{V} and V respectively denote:

$$\begin{pmatrix} X & \bar{Y} \\ Z & \bar{T} \end{pmatrix} \quad (\text{resp. } \begin{pmatrix} \bar{X} & Y \\ \bar{Z} & T \end{pmatrix}) \quad \text{and} \quad \begin{pmatrix} X & Y \\ Z & T \end{pmatrix}$$

where $\bar{Y} = (Y-X)/2$ and $\bar{T} = (T-Z)/2$ (resp. $\bar{X} = (X-Y)/2$ and $\bar{Z} = (Z-T)/2$), then the following are equivalent:

- (1) \bar{V} is in P_i , and $V \cdot V^{\delta \tau}$ commutes with M .
- (2) \bar{V} is in P_i and $V \cdot U \cdot V^{\delta \tau}$ (resp. $V \cdot L \cdot V^{\delta \tau}$) = W^i for some odd i .
- (3) B, C, Z and T satisfy conditions (a) through (d) of Prop.9.1(i) subject to $T > Z > 0$ (resp. $Z > T > 0$).
- (4) B, C, X and Y satisfy conditions (a) through (d) of Cor.9.1.1(i) subject to $Y > X > 0$ (resp. $X > Y > 0$).
- (5) \bar{V} is in P_i , and $\begin{pmatrix} a & C \\ B & a \end{pmatrix} = V^{-1}MV$.

Proof: The proof is similar to the proof of Cor.8.1.1. It will be convenient to suppose that $w(M)$ is an odd-u palindrome; the odd-l case can be treated in essentially the same manner.

(1) \Leftrightarrow (2):

Using the identity $XT - YZ = 2$, and the definitions of \bar{Y} and \bar{T} :

$$\begin{pmatrix} X & \bar{Y} \\ Z & \bar{T} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \bar{T} & \bar{Y} \\ Z & X \end{pmatrix} = \begin{pmatrix} 1+YZ & XY \\ ZT & 1+YZ \end{pmatrix}$$

whence $V.V^{\delta\tau} = D.\bar{V}.U.\bar{V}^{\delta\tau}$, where D is the diagonal matrix $\langle 2, 2 \rangle$. Thus conditions (1) and (2) are equivalent by Thm. 6.4, since D commutes with all matrices in P .

(2) and (3) are proved equivalent in the proof of Prop.9.1, and essentially the same argument can be used to establish the equivalence of (2) and (4).

(2) \Rightarrow (5):

From the proof of Prop.9.1 the relation $bZT = cXY$ holds, whilst

$$Z(bT^2 - cY^2) = 2cY = 2CZ$$

showing that $2C = bT^2 - cY^2$. Similarly $2B = cX^2 - bZ^2$. With the aid of these relations, (5) can be verified by direct computation.

(5) \Rightarrow (1):

Applying the anti-homomorphism $\delta\tau$ to (4) shows that:

$$M = (V^{\delta\tau})^{-1} \begin{pmatrix} a & C \\ B & a \end{pmatrix} V^{\delta\tau}$$

whence $V.V^{\delta\tau}$ commutes with M .

Cor. 9.1.3: Suppose that M is as in Prop. 9.1, and that $w(M)$ is an odd palindrome. If B and C are as in Prop.9.1(ii), and V and D respectively denote $V(M)$ and diagonal matrix $\langle 2, 2 \rangle$, then:

(i) $W(M) = D^{-1}.V.V^{\delta\tau}$

(ii) $M = (V^{\tau})^{-1} \begin{pmatrix} a & B \\ C & a \end{pmatrix} V^{\tau}$

(iii) $\sqrt{B/C}$ has the encoding $\langle f \rangle$, where $F = \text{cap}(f) = D^{-1}.V^{\tau}.V^{\delta}$.

Proof: As in the previous proof, $w(M)$ is assumed to be an odd-u palindrome.

(i) By Prop.9.1 and Cor.9.1.2, the equivalent conditions of Cor.9.1.2 are satisfied with $\bar{V} = V_u$, and (i) follows from the proof of Cor.9.1.2.

(ii) Condition (5) of Cor.9.1.2 is satisfied with $\bar{V} = V_u$, and (ii) is obtained directly by applying τ .

(iii) The argument used to prove that (5) implies (1) in Cor.9.1.2 applies, and establishes that $(V^{\tau}).(V^{\delta})$ commutes with the matrix:

$$\begin{pmatrix} a & B \\ C & a \end{pmatrix}$$

Since $\det V = 2$, direct computation shows that all entries of $V^{\tau}.V^{\delta}$ are even, and that F is in P_i . This proves (iii), since D commutes with all matrices.

Cor.9.1.3 is only a partial analogue of Cor.8.1.2, and the proof cannot be extended (compare the proof of Cor.8.1.2) to obtain an explicit form for $\sqrt{B/C}$, since V^{τ} is not necessarily of the form $V(N)$. In fact, the string f in Cor.9.1.3 may be expressible as g^r with $r > 1$, and the encoding of $\sqrt{B/C}$ may be even, odd-l or odd-u palindromic, as the examples below show.

Example A:

Adopting the notation of Prop.9.1, take $a=k+1$, $b=k$, and $c=1$, where $k>1$. Note that M is in P , so that $W(M)=M$ by Cor.6.4.1(iii), whence $W(M) = U^k L U^k$ by an easy induction. In this case, $B=k+2$ and $C=k$ satisfy the conditions of Prop.9.1(i), since $(k+2) \cdot 1^2 - k \cdot 1^2 = 2$. By Prop.9.1(iii),

$$V = V(M) = \begin{pmatrix} k+2 & k \\ 1 & 1 \end{pmatrix}$$

and, using Cor.9.1.2, the expansion of $\sqrt{B/C}$ has the encoding $\langle f \rangle$, where $\text{cap}(f) = F = D^{-1} \cdot V^T \cdot V^d$. From this relation, F can be directly computed, and proven equal to $U L^k U$ by induction.

Example B:

Let m and n be positive integers, where n is odd and at least 3. In the notation of Prop.9.1, let $a = mn-1$, $b = m(mn-2)$ and $c = n$.

As in the previous example, M is in P , so that $M=W(M)$. Moreover:

$$m \cdot n^2 - (mn^2 - 2n) \cdot 1^2 = 2n,$$

whilst n divides both mn and $mn^2 - 2n$, and $n-1$ and $mn-mn^2+2n$ are both even, so that the conditions of Prop.9.1(i) are satisfied with $B=m$ and $C=(mn-2)n$. If $n=2r+1$, then the matrix defined in Prop.9.1(iii) is

$$V_n = \begin{pmatrix} m & mr-1 \\ 1 & r \end{pmatrix}$$

and an easy inductive argument proves that $V_n = U^{n-1} L U^{r-1}$, so that $\sqrt{B/C}$ has the encoding $\langle u^{n-1} l u^{n-2} l u^{n-3} \dots \rangle$.

The encoding of $\sqrt{B/C}$ is described by the matrix F , as in Cor.9.1.2(iii), which (by Cor.6.4.1(iii)) is in fact the matrix:

$$\begin{pmatrix} a & B \\ C & a \end{pmatrix}$$

A simple inductive argument then proves that $F = L^{n-1} U L^{n-2} U L^{n-3}$.

Thus, $\sqrt{B/C}$ has an odd-1 encoding if m is odd, and an even encoding if m is even and differs from $2n$. In the exceptional case $m=2n$, the encoding of $\sqrt{B/C}$ is $\langle 1^{n-1} u l^{n-1} \rangle$, an odd-u palindromic encoding.

The special cases $B=b$ and $C=c$, or $B=c$ and $C=b$, provide particularly simple instances illustrating Cor.9.1.3, and correspond to the conditions " $V(M) = V(M)^T$ " and " $V(M) = V(M)^d$ " respectively. They occur in particular if $c=1$, and b is a prime of the form $4n+3$, when the two cases are respectively associated with residues 3 and 7 modulo 8. (See Cor.10.1.2). In these cases, the corresponding encodings also have relatively simple forms, in some respects akin to the special forms considered in Cor.8.1.5. A few preliminary definitions are required:

Consider the Raney transducer $RT(2)$ (see §5). $RT(2)$ has two states, D and H , corresponding to the diagonal matrices $\langle 2, 1 \rangle$ and $\langle 1, 2 \rangle$ respectively, which are respectively associated with the transformations which double and halve the value of input encodings.

Definition: An element w of A^* is an acceptable input for state D (resp. H) if $RT(2)$, in responding to input w when initially in state D (resp. H), gives an output after the the last symbol of w is input. Provided that w is an acceptable input for state D (resp. H) of $RT(2)$, the notation $2w$ (resp. $(1/2)w$) will be used for the associated output string.

Lemma 9.2:

Let w be in A^* , and let $W = \text{cap}(w)$. Then:

(i) w is an acceptable input for state D (resp. H) of RT(2) iff

$$W = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ where } cd \text{ (resp. } ab) \text{ is even}$$

$$(ii) W = \begin{pmatrix} a & b \\ 2c & d \end{pmatrix} \text{ iff } \text{cap}(2w) = \begin{pmatrix} a & 2b \\ c & d \end{pmatrix}$$

$$(iii) W = \begin{pmatrix} a & b \\ c & 2d \end{pmatrix} \text{ iff } \text{cap}(2w) = \begin{pmatrix} 2a & b \\ c & d \end{pmatrix}$$

Proof:

The relevant arguments are here presented under the assumption that RT(2) is initially in state D. Similar arguments apply if H is the initial state, and (i), (ii) and (iii) follow directly from the combination of the two cases.

(i) By inspection of RT(2), w is an acceptable input for state D of RT(2) if and only if w is in the regular set:

$$((u^2 + 1)^*(\epsilon + lu(u + 1^2)^*(\epsilon + ul)))^*.$$

By inspection of the Cayley diagram associated with the presentation:

$$\langle u, l : u^2 = l^2 = (ul)^3 = 1 \rangle$$

of $SL(2, \mathbb{Z}_2)$ (see Prop. 7.2), w is an acceptable input which finally transforms RT(2) to state D (resp. H) if and only if c (resp. d) is even.

(ii) and (iii) can be proved using the inductive hypothesis:

" if the initial segment t of w has been input, v has been output, and RT(2) is in state D (resp. H) then

$$T = \text{cap}(t) \text{ has the form } \begin{pmatrix} a & b \\ 2c & d \end{pmatrix} \text{ (resp. } \begin{pmatrix} a & b \\ c & 2d \end{pmatrix})$$

$$\text{and } V = \text{cap}(v) \text{ has the form } \begin{pmatrix} a & 2b \\ c & d \end{pmatrix} \text{ (resp. } \begin{pmatrix} 2a & b \\ c & d \end{pmatrix}) "$$

It suffices to verify directly that the inductive hypothesis remains valid under each appropriate subsequent transition of RT(2). For instance:

$$\begin{pmatrix} a & b \\ 2c & d \end{pmatrix} U = \begin{pmatrix} a & a+b \\ 2c & 2c+d \end{pmatrix}$$

$$\text{whilst } \begin{pmatrix} a & 2b \\ c & d \end{pmatrix} U^2 = \begin{pmatrix} a & 2(a+b) \\ c & 2c+d \end{pmatrix}$$

showing that the inductive hypothesis remains valid after the transition $u:u^2$ from D to D. The corresponding verifications for other transitions are similar, and are omitted.

Cor. 9.1.4:

Let M be as in Prop. 9.1, and $w(M)$ an odd palindrome. If (B, C) is as in Prop. 9.1(ii), and V denotes $V(M)$, then the following are equivalent:

(a) $B=b$ and $C=c$

(b) $V = V^T$

(c) either $w(M)$ is odd- u , and

$Q = L^{-1}V$ is in P_1 , where $q = \text{cap}^{-1}(Q)$ satisfies $q = (1/2)\text{rev}(\text{int}(q))$,
or $w(M)$ is odd- l , and

$Q = U^{-1}V$ is in P_1 , where $q = \text{cap}^{-1}(Q)$ satisfies $q = 2\text{rev}(\text{int}(q))$.

Proof:

(a) and (b) are equivalent in view of Cor. 9.1.3 (i) and (iii).

To see that (b) and (c) are equivalent, assume that $w(M)$ is odd- u . In the notation of Cor. 9.1.2:

$$V = V^T \text{ iff } Y = 2\bar{Y} + X = Z$$

$$\text{iff } Z - X = 2\bar{Y}$$

$$\text{iff } V_u = LQ \text{ where } Q \text{ has the form}$$

$$\begin{pmatrix} p & q \\ 2q & r \end{pmatrix} \text{ by Cor. 2.2.1}$$

$$\text{iff } V_u = LQ \text{ where } q = \text{cap}(Q) \text{ satisfies}$$

$$q = (1/2)\text{rev}(\text{int}(q))$$

by Lemmas 5.2 and 9.2.

A similar argument applies if $w(M)$ is odd- l .

Cor. 9.1.5:

Let M be as in Prop.9.1, and $w(M)$ an odd palindrome. If (B,C) is as in Prop.9.1(ii), and V denotes $V(M)$, then the following are equivalent:

(a) $E=c$ and $C=b$

(b) $V = V^{\delta\tau}$

(c) either $w(M)$ is odd-1, and

$Q = L^{-1}V$ is in P_1 , where $q = \text{cap}^{-1}(Q)$ satisfies $q = (1/2)\text{rev}(q)$,
or $w(M)$ is odd-u, and

$Q = U^{-1}V$ is in P_1 , where $q = \text{cap}^{-1}(Q)$ satisfies $q = 2\text{rev}(q)$.

Proof:

(a) and (b) are equivalent by Cor. 9.1.3 (i) and (iii), and Lemma 5.2.

To see that (b) and (c) are equivalent, assume that $w(M)$ is odd-u. In the notation of Cor.9.1.2:

$V = V^{\delta\tau}$ iff $T = 2\bar{T} + Z = X$

iff $X - Z = 2\bar{T}$

iff $V_u = UQ$ where Q has the form

$\begin{pmatrix} 2r & p \\ q & r \end{pmatrix}$ by Cor.2.2.1

iff $V_u = UQ$ where $q = \text{cap}(Q)$ satisfies
 $q = 2\text{rev}(q)$

by Lemmas 5.2 and 9.2.

A similar argument applies if $w(M)$ is odd-1.

\$10. Some number-theoretic consequences.

The results of \$'s 3 and 9 can be used to give more information about the continued fraction expansions of certain quadratic irrationals. A number of results of this type are grouped together in this section as corollaries to Proposition 10.1, which is a direct consequence of Prop.'s 8.1 and 9.1. This is a convenient way of presenting a set of small and diverse results, but the logical relationship to Proposition 10.1 is often indirect.

Proposition 10.1:

If b and c are positive integers, and bc is not a square, then:

either

(E) there are positive integers B, C, Z and T , with $BC=bc$, such that

(E1): $BT^2 - CZ^2 = c$ where $B \neq c$

and (E2): c divides both BT and CZ

or

(O) there are positive integers B, C, Z and T , with $BC=bc$, such that

(O1): $BT^2 - CZ^2 = 2c$

(O2): c divides both BT and CZ

and (O3): $T-Z$ and $(BT-CZ)/c$ are both even

but only one of the sets of conditions (E) and (O) can be satisfied.

Whichever case applies, B and C are uniquely determined, and there are infinitely many associated values of Z and T satisfying the appropriate set of conditions.

Proof: $\sqrt{b/c}$ either has an odd or even encoding, and one - but only one - of Propositions 8.1 and 9.1 applies.

Remark:

If case (E) applies, then $\gcd(T, Z) = 1$.

If case (O) applies, then $\gcd(T, Z)$ is either 1 or 2. If moreover c is odd, then T and Z are necessarily both odd, and $\gcd(T, Z) = 1$.

Cor. 10.1.1:

Let b and c be positive integers, where b is even, and c is odd. Then:

(i) if $b = 2, 4$ or $6(4)$, then $\sqrt{b/c}$ has an even palindromic encoding.

(ii) if $b \neq 0(32)$, and $\sqrt{b/c}$ has an odd palindromic encoding, then $\sqrt{b/4c}$ has an even palindromic encoding.

Proof:

It will be convenient to prove (i) and (ii) together.

Suppose that $\sqrt{b/c}$ has an odd palindromic encoding. By Prop. 9.1, and the remark above, there is a solution of the equation:

$$BT^2 - CZ^2 = 2c$$

with $BC=bc$ such that T and Z are both odd, and BT and CZ have the same parity. This ensures that both B and C are even, proving that $bc=BC=0(4)$, whence $b=0(4)$. Furthermore:

$$(B/2)T^2 - (C/2)Z^2 = c \dots\dots\dots (*)$$

Since c, T and Z are odd, it now follows that $B/2$ or $C/2$ is even, proving that $BC=0(8)$ and $b=0(8)$.

By Prop. 8.1, the solubility of (*) ensures that $\sqrt{b/4c}$ has an even palindromic encoding unless $B/2=c$, in which case (*) reduces to:

$$cT^2 - (b/4)Z^2 = c.$$

Taking congruences modulo 8 then shows that $b/4$ is divisible by 8, proving that $b=0(32)$.

Remark:

The condition $b=0(8)$ is not sufficient to ensure that $\sqrt{b/c}$ has an odd encoding. For example, $\sqrt{56}$ has the even encoding $\langle u^7 l^2 u^7 \rangle$.

Both $\sqrt{b/c}$ and $\sqrt{b/4c}$ can have odd encodings. For instance:

$\sqrt{96}$ and $\sqrt{24}$ have the encodings $\langle u^7 l u^3 l u^7 \rangle$ and $\langle u^4 l u^4 \rangle$ respectively.

The results of §'s 8 and 9 provide a simple classification of encodings of numbers of the form \sqrt{p} , where p is prime.

Cor. 10.1.2: Let p be prime. Then:

- (i) $\overline{p} = 1(4)$ $\Leftrightarrow \sqrt{p}$ has an even encoding
 $\Leftrightarrow pT^2 - Z^2 = 1$ is soluble in positive integers.
- (ii) $p = 3(8)$ $\Leftrightarrow \sqrt{p}$ has an odd-1 encoding
 $\Leftrightarrow pT^2 - Z^2 = 2$ is soluble in positive integers.
- (iii) $p = 7(8)$ $\Leftrightarrow \sqrt{p}$ has an odd-u encoding
 $\Leftrightarrow T^2 - pZ^2 = 2$ is soluble in positive integers.

Proof: (i) $p = 1(4) \Rightarrow \sqrt{p}$ has an even encoding, by Cor. 7.2.1
 $\Rightarrow pT^2 - Z^2 = 1$ is soluble in positive integers,
by Prop. 8.1.

(ii) $p = 3(8) \Rightarrow pT^2 - Z^2 = 0, 2, 3, 4, \text{ or } 7(8)$ since $0, 1$ and 4 are the only quadratic residues modulo 8 .

From Prop. 10.1, it then follows that $pT^2 - Z^2 = 2$ has a solution, and $T < Z$, so that \sqrt{p} has an odd-1 encoding.

(iii) $p = 7(8) \Rightarrow pT^2 - Z^2 = 0, 3, 4, 6, \text{ or } 7(8)$ since $0, 1$ and 4 are the only quadratic residues modulo 8 .

From Prop. 10.1, it then follows that $T^2 - pZ^2 = 2$ has a solution, and $T > Z$, so that \sqrt{p} has an odd-u encoding.

To complete the proof, it is enough to observe that the properties of 'having an even/odd-1/odd-u encoding' are mutually exclusive conditions.

Remark:

Cor. 10.1.2 proves some simple properties of the Legendre symbol, viz:

$$\begin{aligned} (-1/p) &= 1 & \text{if } p=1(4) \\ (-2/p) &= 1 & \text{if } p=3(8) \\ (2/p) &= 1 & \text{if } p=7(8) \end{aligned}$$

Such properties of quadratic residues could have been used to give a simpler proof of the corollary, but it is of interest to derive the result from elementary congruences.

Cor. 10.1.3:

Let r and s be co-prime integers. Then $\sqrt{r/s}$ has an encoding of the form $v.\text{rev}(v)$ where $v = \text{rev}(\text{int}(v))$ iff \sqrt{rs} also has an encoding of this form.

Proof:

By Cor. 8.1.5:

$\sqrt{r/s}$ has an encoding of the form $v.\text{rev}(v)$ where $v = \text{rev}(\text{int}(v))$
iff $rT^2 - sZ^2 = s$ has a solution with s dividing rT
iff $rT^2 - sZ^2 = s$ has a solution with s dividing T
iff $rT^2 - Z^2 = 1$ has a solution in positive integers.
iff \sqrt{rs} has a palindromic encoding of the required form.

The above corollary applies in particular to the case where $r=p$ and $s=q$, where p and q are both prime. A related result is:

Cor. 10.1.4:

Let p and q be distinct primes, and suppose that \sqrt{pq} has an even encoding of the form $v.\text{rev}(v)$ where $v \neq \text{rev}(\text{int}(v))$. Then one or other of $\sqrt{p/q}$ and $\sqrt{q/p}$ has the encoding $\text{rev}(v).v$.

Proof: By Prop. 8.1, one or other of the equations:

$$pT^2 - qZ^2 = 1 \text{ or } qT^2 - pZ^2 = 1$$

has a solution in positive integers. The result then follows from Cor. 8.1.2.

The encodings of numbers of the form \sqrt{pq} , where p and q are both prime, can be classified using elementary congruences and properties of the Legendre symbol. (C.f. Cor.10.1.2). Such a classification is presented in tabular form below. The arguments used to construct the table are omitted; they depend only upon trivial congruences modulo 8 and results on the quadratic character of $-1, 2$ and -2 modulo a prime number which are discussed in [D p.66-69].

Table summarising encodings of \sqrt{pq} , where p and q are prime.

p	q	Parity	Equation type	Example of occurrence	(p/q)
2	=1 (8)	even	$2T^2 - qZ^2 = 1$	$q=17, T=3, Z=1$	+1
			$2qT^2 - Z^2 = 1$	$q=41, T=1, Z=9$	
			$qT^2 - 2Z^2 = 1$	$q=73, T=1, Z=6$	
2	=3 (8)	even	$qT^2 - 2Z^2 = 1$	$q=11, T=3, Z=7$	-1
2	=5 (8)	even	$2qT^2 - Z^2 = 1$	$q=5, T=1, Z=3$	-1
2	=7 (8)	even	$2T^2 - qZ^2 = 1$	$q=7, T=2, Z=1$	+1
=1 (4)	=1 (4)	even	$pqT^2 - Z^2 = 1$	$p=5, q=29, T=1, Z=12$	+1
			$pqT^2 - Z^2 = 1$	$p=5, q=13, T=1, Z=8$	-1
			$pT^2 - qZ^2 = 1$	$p=5, q=41, T=63, Z=22$	+1
=1 (4)	=3 (4)	even	$pT^2 - qZ^2 = 1$	$p=13, q=3, T=1, Z=2$	+1
=1 (8)	=3 (8)	odd	$pqT^2 - Z^2 = 2$	$p=17, q=43, T=1, Z=27$	+1
			$pqT^2 - Z^2 = 2$	$p=17, q=3, T=1, Z=7$	-1
			$qT^2 - pZ^2 = 2$	$p=17, q=19, T=1, Z=1$	+1
=1 (8)	=7 (8)	odd	$T^2 - pqZ^2 = 2$	$p=73, q=23, T=41, Z=1$	+1
			$T^2 - pqZ^2 = 2$	$p=17, q=7, T=11, Z=1$	-1
			$pT^2 - qZ^2 = 2$	$p=17, q=47, T=5, Z=3$	+1
=5 (8)	=3 (8)	odd	$pT^2 - qZ^2 = 2$	$p=5, q=3, T=1, Z=1$	-1
=5 (8)	=7 (8)	odd	$qT^2 - pZ^2 = 2$	$p=5, q=7, T=1, Z=1$	-1
=3 (4)	=3 (4)	odd	$pT^2 - qZ^2 = 1$	$p=3, q=11, T=2, Z=1$	+1

In connection with the table, it should be noted that the entries and examples are representative of all the possible conditions which can occur. For example, if $p=q=3(4)$, then reference to the table shows that the canonical equation has just one possible form. Since $(-1/p)=(-1/q)=-1$, a special case of the quadratic reciprocity law can be inferred.

A note on factorisation.

Proposition 10.1 has some connection with the problem of factorisation. Reference to the above table shows, for example, that the factorisation of a product of the form $n=pq$, where p and q are primes of the form $4k+3$, can 'in principle' be computed from the encoding of \sqrt{pq} . It is thus unsurprising that, at least with current techniques, the computation of the periodic part of \sqrt{n} is in general infeasible for large n . Despite this, Proposition 10.1 may be relevant to the theory of factorisation, and does provide the basis for the following factorisation technique which is effective for small integers.

Algorithm 10.2: A heuristic factorisation technique, intended to find a non-trivial factor of a composite integer n .

1. Choose a positive integer multiplier k .
2. Compute the 'first half' of the palindromic period w of the encoding of \sqrt{kn} , i.e. compute v such that $w = v.\text{rev}(v)$, $v.u.\text{rev}(v)$ or $v.l.\text{rev}(v)$ as appropriate.
3. Compute $V = \text{cap}(v)$, and compute B and C using Prop.8.1 or 9.1(iii).
4. Compute $\text{GCD}(B, n)$ to determine whether a non-trivial factor has been obtained.

Notes on Algorithm 10.2.

1. Algorithm 10.2 bears a superficial resemblance to a factorisation technique developed by D.H.Lehmer and R.E.Powers after Legendre, and described and illustrated in [K] p.351, and [BM]. It should be noted that the Lehmer-Powers method may require only a small number of convergents of \sqrt{kn} to obtain a factorisation of n , whilst Algorithm 10.2 could only be of practical interest if alternative methods for computing the continued fraction expansions of quadratic irrationals could be found (see Example 2 below, and [K] p.353). The computational considerations discussed below are thus of academic rather than practical interest, at least at present. In this connection, it should also be noted that the efficient algorithm for deciding the solvability or unsolvability of the equation $X^2 - DY^2 = -1$ described in [L] requires a complete prime factorisation of D as input.

2. As far as the choice of k is concerned, it may be possible in special cases to describe a class of multipliers giving a high probability of factorisation 'in principle'. For instance, if $n=pq$ where p and q are respectively congruent to 1 and 5 modulo 8, then elementary congruences and properties of the Legendre symbol show that if k is a prime of the form $4k+3$ which is not a quadratic residue modulo p , then Algorithm 10.2 'in principle' determines the factorisation of n . If n is large, it seems doubtful whether any choice of k can make the computation of the periodic part of \sqrt{kn} feasible in general (using a standard algorithm). See [L] and [M&B] for a discussion of related topics.

3. The computation of V is naturally carried out in conjunction with the computation of v . Even when n is small, the computation of V may involve calculations with enormous integers. (If the encoding of v has $2r$ or more exponents, then the matrix V has entries at least as large as the r -th Fibonacci number.) Since B and C are determined exactly if computed modulo a base $p > n$, it is expedient to compute the entries of V modulo a suitably large base p . Since B and C are typically determined from equations of the form $B = x/t$, $C = y/z$ where x, y, z and t are computed without using division, a base p is suitable provided that $\text{GCD}(p, t) = \text{GCD}(p, z) = 1$. Any risk of failure on account of non-trivial GCD's can be overcome by performing calculations modulo a number of primes and using Chinese-remaindering techniques, or working modulo n itself. The effectiveness of working modulo n can be illustrated under the assumption that \sqrt{n} has an even encoding. In that event, Prop.8.1 shows that

$$C = Y/Z \text{ where } BC=bc \text{ and } BT^2 - CZ^2 = 1.$$

Since B and Z are coprime and $B=1$, it is impossible for n to divide Z , and either Z has a multiplicative inverse modulo n , or $\text{GCD}(n, Z)$ is a non-trivial factor of n . (Similar arguments apply if \sqrt{n} has an odd encoding.)

Illustrative examples:

The matrix V , computed at step 3 in Algorithm 10.2, will be denoted by:

$$\begin{pmatrix} X & Y \\ Z & T \end{pmatrix}$$

The notation is otherwise as in Algorithm 10.2.

Example 1:

Let n be 11111 and take $k = 1$. The exponents of the encoding of \sqrt{n} are:

105, 2, 2, 4, 5, 2, 7, 1, 41, 3, 1, 1, 4, 1, 1, 3, 41, 1, 7, 2, 5, 4, 2, 2, 105

- an even encoding - and the coefficients of V are as follows:

$X = 66303355$, $Y = 170462252$, $Z = 629012$, $T = 1617155$.

By Prop. 8.1, $B = X/T = 41$, and $C = Y/Z = 271$, whence $n = 41.271$.

Example 2:

Let $n = 197209$ and take $k=1$. The continued fraction expansion of \sqrt{n} in this case has 776 terms and an even encoding, and the coefficients of V are computed modulo the prime $p = 274877906899$ as follows:

$X = 120484871765$, $Y = 124264692107$, $Z = 7337124391$, $T = 185699117569$.

The multiplicative inverse of T modulo p is 160817613058, and that of Z is 62360244984, and B and C are computed modulo p as 199 and 991 respectively.

Example 3:

Let $n = 324851$. A few possible choices of multiplier k are considered, by way of illustration, and the straightforward numerical calculations are suppressed.

Taking $k=1$ leads to a continued fraction expansion of 46 terms, which has an odd-1 encoding. The string v here has the exponents:

569, 1, 22, 3, 1, 3, 1, 1, 2, 1, 1, 3, 2, 1, 1, 3, 2, 3, 1, 1, 7, 11, 2, 284

which is easily seen to have the characteristics described in Cor. 9.1.6.(iii). Indeed, there is no non-trivial factorisation of n in this case.

Taking $k=2$ and $k=3$ leads to expansions of numerical length 114 and 40 respectively. In both cases, the resulting factorisation is trivial; if $k=2$, then $B = 324851$ and $C = 2$, whilst if $k=3$, then $B = 3$, and $C = 324851$.

Choosing $k=5$ leads to an expansion of numerical length 72 which has an odd- u encoding, and v has the sequence of exponents:

1274, 2, 6, 5, 3, 1, 7, 5, 1, 1, 2, 2, 1, 1, 36, 2, 1, 4,

1, 1, 2, 1, 4, 1, 23, 4, 1, 1, 13, 1, 1, 8, 1, 1, 1, 1.

In this case, $B=577$, and n factorises as 563.577 .

Example 4:

Let n be the Fermat number $F_5 = 4294967297$. In this case, $k=1$ is an unsuitable multiplier, since n is of the form r^2+1 and \sqrt{n} has the expansion $[r; 2r, 2r, \dots]$, with a numerical period of odd length. Taking $k=10$ leads to a continued fraction expansion of length 1816 for \sqrt{kn} , corresponding to an even encoding. In this case, $B = 641$, and the factorisation of n as 641.6700417 is obtained.

Concluding remarks:

The literature on quadratic forms is so vast that it is difficult to assess the extent to which the results of the later sections of this paper have been explicitly or implicitly anticipated.

The derivation of Pell's equation following Prop.7.1 is clearly connected with the classical relationship between Pell's equation and automorphisms of forms of given discriminant (see e.g. Gauss [G] Art.162). There are also parallels between Theorem 6.4 and the study of periods of reduced forms of positive discriminant D as described in [G] Art's 185-188.

The results of Prop.8.1 and 9.1 seem to be related to the study of the 2-component of the group of equivalence classes of binary quadratic forms with a fixed positive discriminant (see e.g. Cassels [C] Chapter 14, Section 6). The latter topic has been studied by Shanks in connection with a theory of factorisation (see [SH]).

References.

- [BM] A method of factoring and the factorisation of F_q .
J.Brillhart and M.A.Morrison Math.Comp. 29(1975),183-205.
- [C] Rational Quadratic Forms.
J.W.S.Cassels Academic Press, 1978.
- [CH] Algebra, an Elementary Text-book, Vol.2.
G.Chrystal Chelsea, 7th. edition, 1964.
- [D] The Higher Arithmetic.
H.Davenport Hutchinson, 3rd. edition, 1968.
- [Di] A Discipline of Programming.
E.W.Dijkstra Prentice-Hall, 1976.
- [G] Disquisitiones Arithmeticae, 1801; English translation.
C.F.Gauss (trans. A.A.Clarke) Yale U.P., 1966.
- [K] The Art of Computer Programming: Vol.2.
D.E.Knuth Addison Wesley, 1969.
- [L] On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$.
J.C.Lagarias Trans.Amer.Math.Soc. 260(2), 485-507, 1980.
- [R] On continued fractions and finite automata.
G.N.Raney Math.Ann. 206(1973),265-283.
- [SH] Class number, a theory of factorisation, and genera.
D.Shanks Proc.Symp.Pure Math. 20(1971), 415-440.

Appendix 1:

Suppose that M is an arbitrary 2×2 integer matrix with integer entries, and that x is a (finite) non-zero real number. (The easy special cases $x = -\infty, 0$ or $+\infty$ can be dealt with separately). The algorithm outlined below, which differs from that given by Raney in [R] only in minor respects, can be used to reduce the computation of $M[x]$ to a computation of $N[y]$ where N is in P and y is in \mathbb{R}^{∞} . At each step in the algorithm, M and x are transformed in such a way that successive values of $M[x]$ are simply related.

{ $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ initially, and $x = [x_0, x_1, x_2, \dots]$ where x_0 may be < 0 .

In the sequel, a, b, c, d will be used to denote the appropriate current entries in the array M }

if $\det M < 0 \rightarrow M := \begin{pmatrix} b & a \\ d & c \end{pmatrix}; x := 1/x$ fi

{ $(b+a/x)/(d+c/x) = (ax+b)/(cx+d)$ so $M[x]$ unchanged.

$\det M > 0$ is achieved, and $\det M$ is thereafter invariant }

if $x_0 < 0 \rightarrow M := MU^{x_0}; x := x - x_0$ fi

{ $x \geq 0$ is achieved, and $M[x]$ is unchanged by Prop. 2.1 (iii) }

do $cd < 0 \rightarrow$

if $x \leq 1 \rightarrow M := ML; x := x/(1-x)$

if $x \geq 1 \rightarrow M := MU; x := x-1$

fi

od

{ x remains ≥ 0 , and $M[x]$ is unchanged by Prop. 2.1.

Termination of the loop is guaranteed since both c and d are non-zero and the assignments $M := MU$ and $M := ML$ both properly increase the value of the product cd .

This step achieves $cd > 0$ }

if $c < 0$ or $d < 0 \rightarrow M := -M$ fi

{ This step achieves $c \geq 0$ and $d \geq 0$ }

if $d = 0$ and $x \neq 0 \rightarrow$

do $x \leq 1 \rightarrow M := ML; x := x/(1-x)$ od;

$M := M.U; x := x-1$

fi;

{ Since $ad-bc > 0$, there are 3 possible cases prior to this step:

(a) c and d both > 0

(b) $a > 0, d > 0$ and $c = 0$

(c) $b < 0, c > 0$ and $d = 0$

Only in case (c) does the if -clause apply. If $d = x = 0$, then the required result is $-\infty$, otherwise repeated replacement of x by $x/(1-x)$ increases x until ultimately x is at least 1. But then the assignment $M := MU$ ensures $c=d > 0$. Thus this step achieves an M satisfying (a) or (b) without altering $M[x]$. (See Prop. 2.1 (iii) and (iv)) }

$s := 0$;

do $M \notin P \rightarrow M := UM; s := s+1$ od

{ On termination of this loop the required answer is $M[x]-s$, in view of Prop. 2.1 (i).

To prove that termination occurs it is sufficient to observe that adding a suitably large multiple of the row (c,d) to (a,b) will necessarily make a and b non-negative, thereby insuring that M is in P . }

Appendix 2:

The transition diagrams of the Raney transducers RT(2), RT(4) and RT(6) are appended. RT(2) has two states, represented by the matrices:

$$H = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \text{ and } D = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

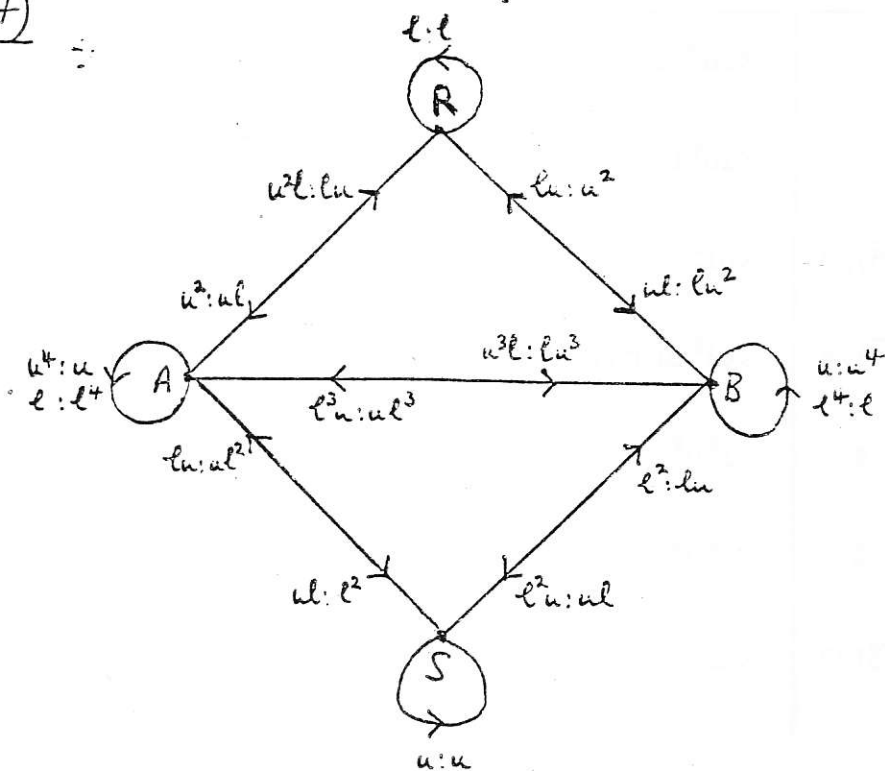
RT(4) has two components, one of which is trivial and comprises the diagonal matrix $\langle 2, 2 \rangle$. The non-trivial component has four states represented by the matrices:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}, B = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}, R = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}, S = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}.$$

RT(2)



RT(4)



Diagrams indicating fixpoint cycles of states in RT(13) and RT(19) are appended (see §6). Only those transitions appearing in a fixpoint cycle are represented in these diagrams, and, for convenience, fixpoint cycles are superimposed on a single diagram where appropriate.

The following tables record representative subsets of the encodings which arise as fixpoints in these cases:

Table for RT(13):

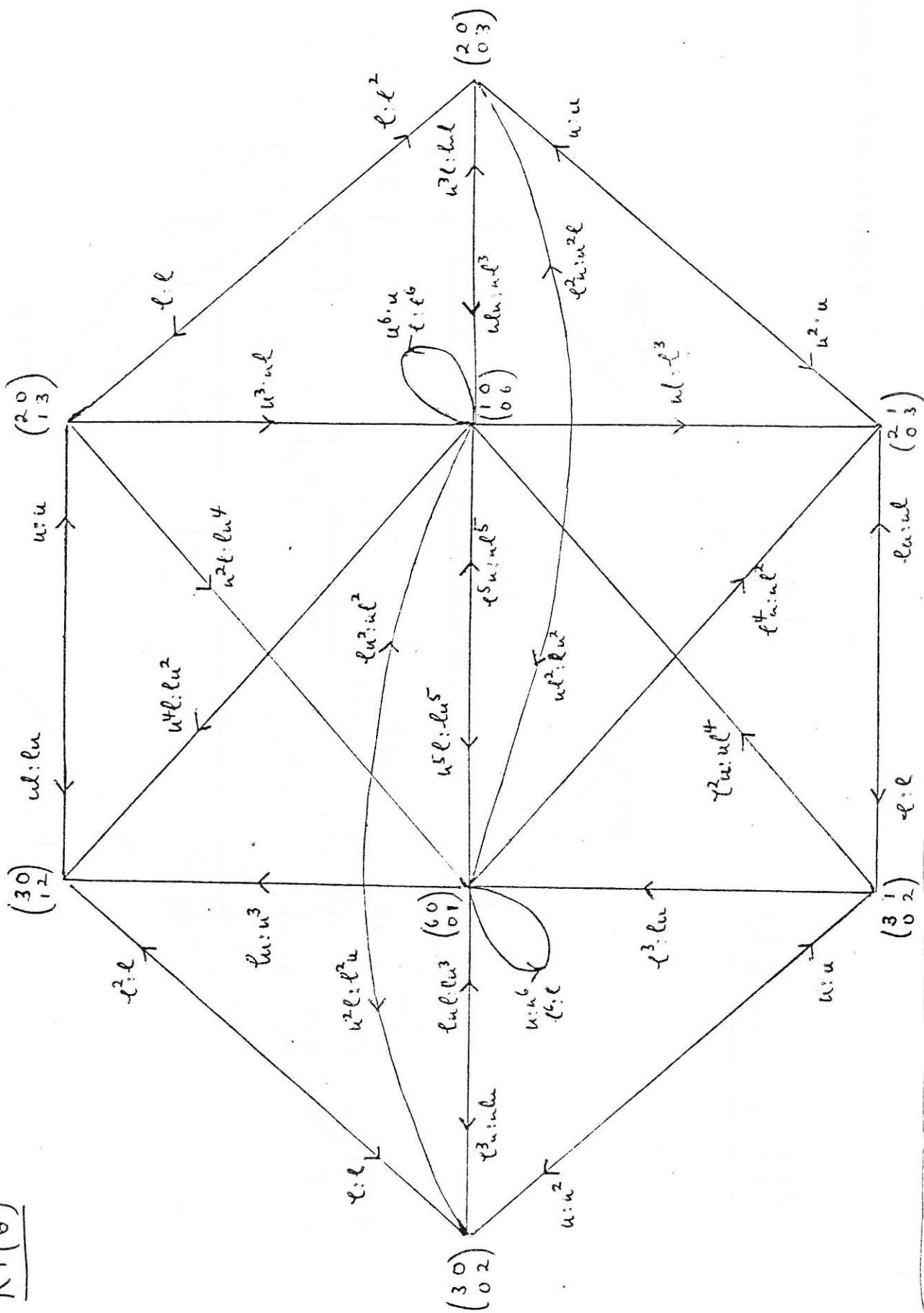
State	Fixpoint	Encoding
$\begin{pmatrix} 4 & 3 \\ 1 & 4 \end{pmatrix}$	$\sqrt{3}$	$\langle ulu \rangle$
$\begin{pmatrix} 3 & 2 \\ 1 & 5 \end{pmatrix}$	$\sqrt{3} - 1$	$\langle lu^2 \rangle$
$\begin{pmatrix} 2 & 1 \\ 1 & 7 \end{pmatrix}$	$(\sqrt{29}-5)/2$	$\langle l^5 u^5 \rangle$
$\begin{pmatrix} 5 & 3 \\ 4 & 5 \end{pmatrix}$	$\sqrt{3}/2$	$\langle lu^6 l \rangle$

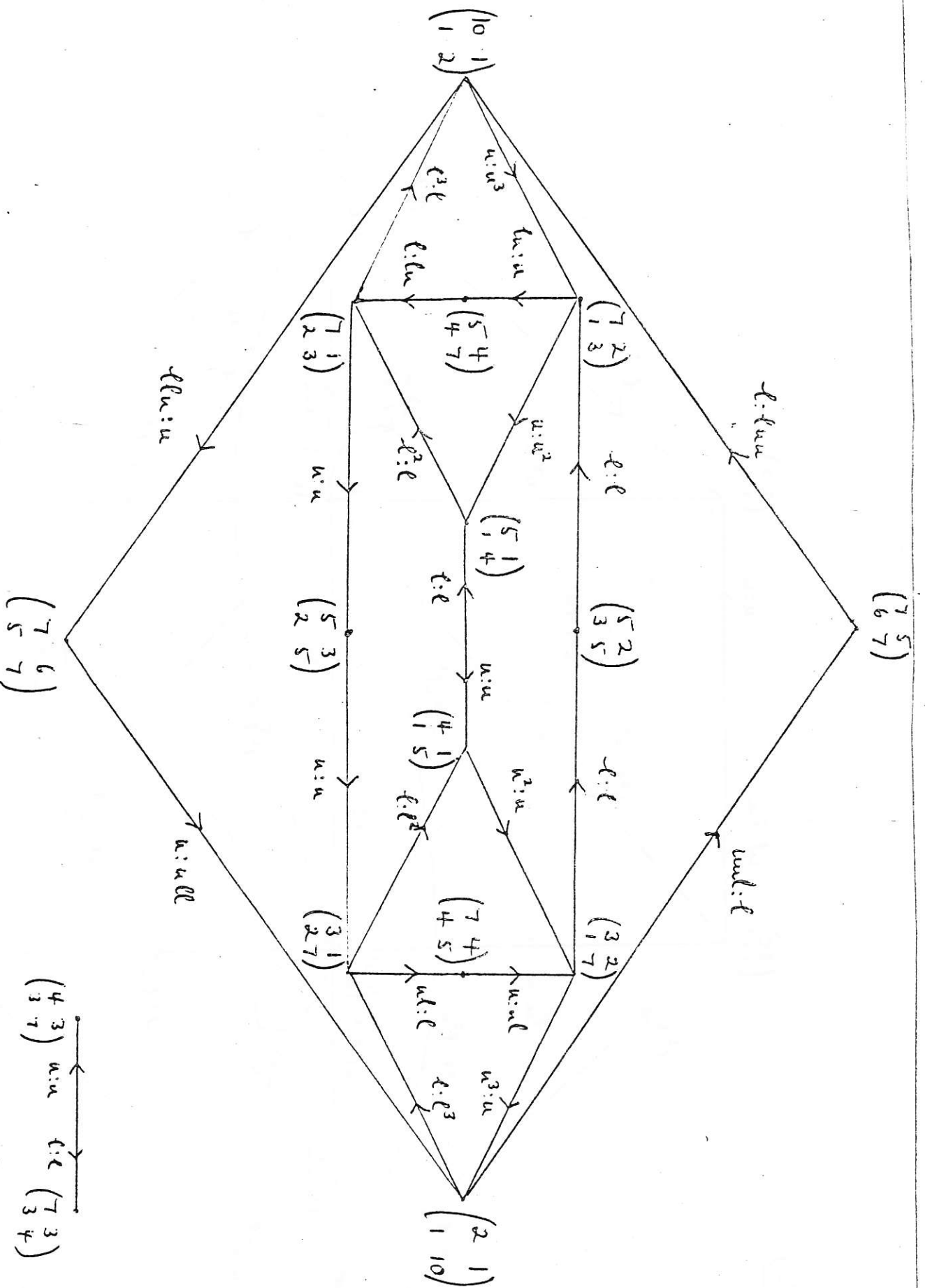
Table for RT(19):

State	Fixpoint	Encoding
$\begin{pmatrix} 7 & 5 \\ 6 & 7 \end{pmatrix}$	$\sqrt{5/6}$	$\langle lu^{10} l \rangle$
$\begin{pmatrix} 5 & 2 \\ 3 & 5 \end{pmatrix}$	$\sqrt{2/3}$	$\langle lu^4 l \rangle$
$\begin{pmatrix} 5 & 1 \\ 1 & 4 \end{pmatrix}$	$(1+\sqrt{5})/2$	$\langle ul \rangle$
$\begin{pmatrix} 7 & 4 \\ 4 & 5 \end{pmatrix}$	$(1+\sqrt{17})/4$	$\langle ul^3 ulu^2 l \rangle$
$\begin{pmatrix} 2 & 1 \\ 1 & 10 \end{pmatrix}$	$\sqrt{17} - 4$	$\langle l^8 u^3 \rangle$
$\begin{pmatrix} 3 & 2 \\ 1 & 7 \end{pmatrix}$	$\sqrt{6} - 2$	$\langle l^2 u^4 \rangle$
$\begin{pmatrix} 7 & 3 \\ 3 & 4 \end{pmatrix}$	$(1+\sqrt{5})/2$	$\langle ul \rangle$

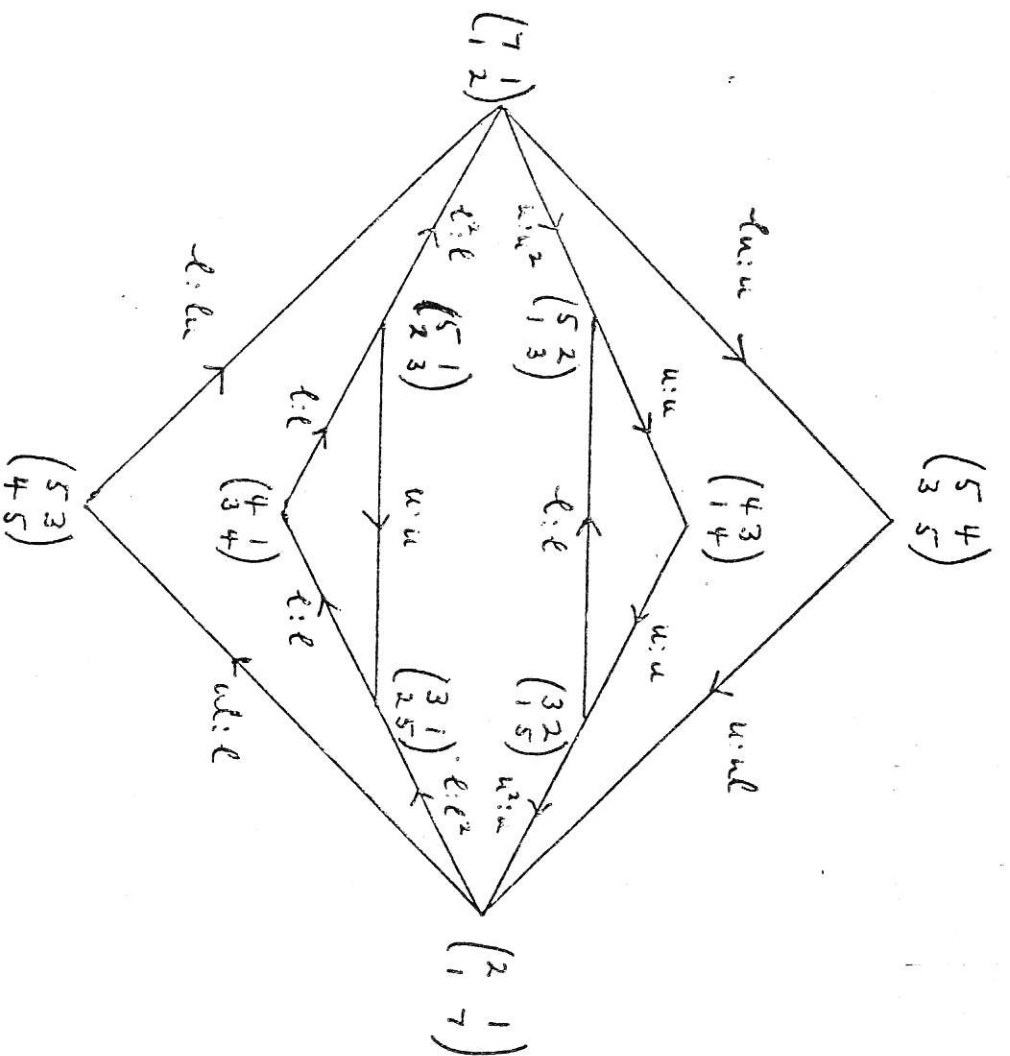
The diagram is a directed graph with the following nodes and edges:

- Nodes:**
 - (30) (top left)
 - (20) (top right)
 - (10) (center)
 - (03) (bottom right)
 - (30) (bottom left)
 - (20) (bottom center)
 - (10) (bottom center)
 - (03) (bottom left)
 - (30) (bottom right)
 - (20) (bottom left)
- Edges and Labels:**
 - $(30) \rightarrow (20)$: $u:u$
 - $(20) \rightarrow (10)$: $l:l$
 - $(10) \rightarrow (03)$: $u^3:u^3$
 - $(03) \rightarrow (30)$: $l:l$
 - $(30) \rightarrow (20)$: $u^2:l$
 - $(20) \rightarrow (10)$: $l^2:l^2$
 - $(10) \rightarrow (03)$: $u^2:u^2$
 - $(03) \rightarrow (30)$: $l^2:l^2$
 - $(30) \rightarrow (20)$: $u^4:l^2$
 - $(20) \rightarrow (10)$: $l^4:l^4$
 - $(10) \rightarrow (03)$: $u^4:u^4$
 - $(03) \rightarrow (30)$: $l^4:l^4$
 - $(30) \rightarrow (20)$: $u^5:l^3$
 - $(20) \rightarrow (10)$: $l^5:l^5$
 - $(10) \rightarrow (03)$: $u^5:u^5$
 - $(03) \rightarrow (30)$: $l^5:l^5$
 - $(30) \rightarrow (20)$: $u^6:l^4$
 - $(20) \rightarrow (10)$: $l^6:l^6$
 - $(10) \rightarrow (03)$: $u^6:u^6$
 - $(03) \rightarrow (30)$: $l^6:l^6$





Fixpoint cycles in RT(19).



Fixpoint cycles in $RT(13)$.